

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-307055
 (43)Date of publication of application : 02.11.2001

(51)Int.Cl.
 G06K 19/073
 B42D 15/10
 G06K 17/00
 G06K 19/07
 G06K 19/00

(21)Application number : 2000-388796 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
 (22)Date of filing : 21.12.2000 (72)Inventor : TAMAI SEIICHIRO
 DOSAKA SHINICHI

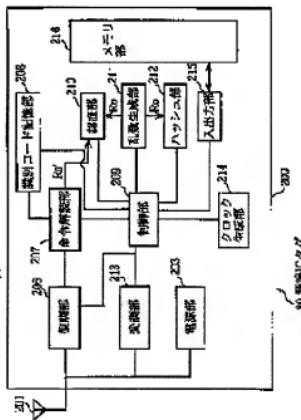
(30)Priority
 Priority number : 11373880 Priority date : 28.12.1999 Priority country : JP
 2000037134 15.02.2000 JP

(54) INFORMATION STORAGE MEDIUM, NON-CONTACT IC TAG, ACCESS DEVICE, ACCESS SYSTEM, LIFE CYCLE MANAGEMENT SYSTEM, INPUT /OUTPUT METHOD AND ACCESSING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a non-contact IC tag to store secret information by every stages in a life cycle from production to abolishment and an access device capable of secretly reading/wiring information to the non-contact IC tag by each stage.

SOLUTION: A memory part 216 is provided with the same number of stage storage areas as the number of stages, each stage storage area is identified by a secret stage identifier, a control part 209 secretly receives an access identifier from the access device via an antenna part 201, a switching part, an impedance switching part, a demodulating part 206 and an instruction decoding part 207, decides whether the secretly received access identifier correctly identifies one of the stage storage areas, receives access information from the access device when it is decided that correct identification of a single stage storage area is made and an input/output part accesses the stage storage area based on the received access information.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-307055

(P2001-307055A)

(43)公開日 平成13年11月2日 (2001.11.2)

(51)Inventor's name	識別記号	F 1	マイコード(参考)
G 0 6 K 19/073		B 4 2 D 15/10	5 2 1 2 C 0 0 5
B 4 2 D 15/10	5 2 1	G 0 6 K 17/00	F 5 B 0 3 5
G 0 6 K 17/00			L 5 B 0 5 8
			E
		19/00	P
審査請求 未請求 請求項の数25 O.L (全 43 頁)			最終頁に続く

(21)出願番号	特願2000-388796(P2000-388796)	(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成12年12月21日 (2000.12.21)	(72)発明者	玉井 誠一郎 大阪府高槻市幸町1番1号 松下電子工業 株式会社内
(31)優先権主張番号	特願平11-373880	(72)発明者	道阪 伸一 大阪府高槻市幸町1番1号 松下電子工業 株式会社内
(32)優先日	平成11年12月28日 (1999.12.28)	(74)代理人	100090446 弁理士 中島 司朗
(33)優先権主張国	日本 (JP)		
(31)優先権主張番号	特願2000-37134(P2000-37134)		
(32)優先日	平成12年2月15日 (2000.2.15)		
(33)優先権主張国	日本 (JP)		

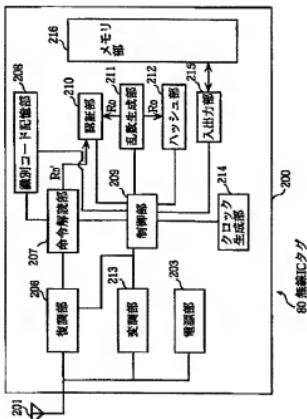
最終頁に続く

(54)【発明の名称】 情報記憶媒体、非接触ICタグ、アクセス装置、アクセスシステム、ライフサイクル管理システム、入出力方法及びアクセス方法

(57)【要約】

【課題】 生産から廃棄に至るまでのライフサイクルにおける複数のステージ毎に秘密の情報を記憶する非接触ICタグと非接触ICタグに対してステージ毎に秘密に情報を読み書きできるアクセス装置とを提供する。

【解決手段】 メモリ部216は、ステージ数と同数のステージ記憶領域を有し、各ステージ記憶領域は、秘密のステージ識別子により識別され、制御部209は、アンテナ部201、切換部、インピーダンス切換部、復調部206、命令解読部207を介して、アクセス識別子をアクセス装置から秘密に受信し、秘密に受信した前記アクセス識別子が前記複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別するか否かを判断し、正しく識別すると判断される場合に、前記アクセス装置からアクセス情報を受信し、入出力部は、受信したアクセス情報に基づいて、ステージ記憶領域へのアクセスを行う。



【特許請求の範囲】

【請求項1】 不揮発性メモリを有し、電波を用いて非接触に読み書き可能な情報記憶媒体であって、複数の記憶領域を有する記憶手段と、各記憶領域を識別する領域識別子を格納している格納手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記格納手段に格納されている領域識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別される記憶領域へのアクセスを行う出入力手段とを備えることを特徴とする情報記憶媒体。

【請求項2】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、

前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、

前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う出入力手段とを備えることを特徴とする非接触ICタグ。

【請求項3】 前記秘密受信手段は、

第1認証子を生成し、生成した第1認証子を前記アクセス手段へ出力する認証子出力手段と、

前記アクセス識別子を暗号化鍵として用いて、出力した前記第1認証子に暗号アルゴリズムが施されて生成された第2認証子を前記アクセス装置から取得する取得手段と、

前記複数のステージ識別子を暗号化鍵として用いて、生成した前記第1認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第3認証子を生成する暗号手段とを含み、

前記判断手段は、取得した第2認証子が生成した複数の第3認証子のうちのいずれか1個と一致するか否かを判断し、一致する場合に、受信した前記アクセス識別子が

前記識別子記憶手段に格納されているステージ識別子の

いずれかと一致すると判断し、

前記出入力手段は、前記アクセス識別子により識別されるステージ記憶領域として、前記第2認証子に一致する第3認証子を生成する際に暗号化鍵として用いられたステージ識別子により識別されるステージ記憶領域へのアクセスを行うことを特徴とする請求項2記載の非接触ICタグ。

【請求項4】 前記認証子出力手段は、ランダムに第1認証子を生成することを特徴とする請求項3記載の非接触ICタグ。

【請求項5】 前記秘密受信手段は、時分割多重された通信チャネルのうち、1個の通信チャネルを選択するチャネル選択手段と、選択された前記通信チャネルを介して、アクセス識別子を秘密に受信する識別子受信手段とを含むことを特徴とする請求項4に記載の非接触ICタグ。

【請求項6】 前記チャネル選択手段は、時分割多重された通信チャネルのうち、1個の通信チャネルをランダムに選択することを特徴とする請求項5に記載の非接触ICタグ。

20 20 ICタグ。

【請求項7】 前記記憶手段は、さらに、共有識別子により識別される共有記憶領域を有し、

前記識別子記憶手段は、さらに、前記共有識別子を記憶しており、

前記判断手段は、さらに、受信した前記アクセス識別子が前記識別子記憶手段に記憶されている共有識別子と一致するか否かを判断し、

前記アクセス情報受信手段は、さらに、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信し、

前記出入力手段は、さらに、受信したアクセス情報に基づいて、前記アクセス識別子により識別される共有記憶領域へのアクセスを行うことを特徴とする請求項2記載の非接触ICタグ。

【請求項8】 前記非接触ICタグが有する不揮発性メモリは、ヒューズメモリであることを特徴とする請求項2記載の非接触ICタグ。

【請求項9】 前記物品の表面に備えられたロゴタイプの近傍に備えられることを特徴とする請求項2に記載の非接触ICタグ。

【請求項10】 前記記憶手段にてデータを記憶する際に、併せて時刻情報を記憶する時刻情報記憶手段を備えることを特徴とする請求項2に記載の非接触ICタグ。

【請求項11】 前記記憶手段は、データを上書きできない第1のメモリ部と、

データを上書きできる第2のメモリ部とを有することを特徴とする請求項2に記載の非接触ICタグ。

【請求項12】 前記記憶手段は、さらに、拡張記憶領域を有し、

50 拡張記憶領域以外の記憶領域において空き容量不足によ

りデータを記憶できないときは、前記拡張記憶領域に記憶することを特徴とする請求項2に記載の非接触ICタグ。

【請求項13】 前記記憶手段が空き容量不足によりデータを記憶できない場合、前記時計情報がもとも古いデータを削除して、空き容量を増加させる記憶整理手段を備えることを特徴とする請求項10に記載の非接触ICタグ。

【請求項14】 マスタ識別子を記憶するマスタ識別子記憶手段と、

受信した前記アクセス識別子が前記マスタ識別子記憶手段に記憶されているマスタ識別子と一致するか否かを判断するマスタ識別子判断手段と、

前記マスタ識別子判断手段が一致すると判断した場合に、前記アクセス装置からマスタアクセス情報を受信するマスタアクセス情報受信手段と、

前記マスタアクセス情報に基づいて、所定のステージ記憶領域へのアクセスを行う入出力手段とを、更に、備えることを特徴とする請求項2に記載の非接触ICタグ。

【請求項15】 入院から退院に至るまでの病院の療養サイクルにおける複数のステージを経由する入院患者に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、前記療養サイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、

受信した前記アクセス識別子が前記識別子記憶手段に記憶しているステージ識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、

受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行いう入出力手段とを備えることを特徴とする非接触ICタグ。

【請求項16】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する高級ブランド品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、

前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、

前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、

受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否

かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段とを備えることを特徴とする非接触ICタグ。

【請求項17】 不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別される複数個の記憶領域を有し、電波を用いて非接触に読み書き可能な情報記憶媒体に対して情報を送受信するアクセス装置であって、アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記情報記憶媒体に対して送信する秘密送信手段と、前記情報記憶媒体により、秘密に送信した前記アクセス識別子が前記情報記憶媒体が有する複数個の記憶領域うちの1個の記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備えることを特徴とするアクセス装置。

20 【請求項18】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されるライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触ICタグに対して情報を送受信するアクセス装置であって、アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記非接触ICタグに対して送信する秘密送信手段と、

前記非接触ICタグにより、秘密に送信した前記アクセス識別子が前記非接触ICタグが有する複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備えることを特徴とするアクセス装置。

【請求項19】 前記非接触ICタグは、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶しており、前記秘密送信手段は、

40 前記非接触ICタグから第1認証子を受信する認証子受信手段と、

前記アクセス識別子を暗号鍵として用いて、受信した前記第1認証子に暗号アルゴリズムを施して第2認証子を生成し、生成した第2認証子を前記非接触ICタグへ出力する認証子出力手段とを備え、

前記アクセス情報送信手段は、前記非接触ICタグにより、前記複数のステージ識別子を暗号化鍵として用いて、前記第1認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第3認証子が生成され、

50 出力された前記第2認証子が生成した複数の第3認証子

を収集し、この情報を利用して物品を管理するアイデアが提案されている。例えば、特開平10-222568号公報によると、ライフサイクル全体での低コスト化を実現するために、製品の製造時、使用時、メンテナンス時に型番・製造番号などの識別情報、材質情報、稼働情報、エラー情報、メンテナンス情報を、各製品、部品毎に入力し、入力された情報を記憶し、記憶された情報を読み出して、製造、メンテナンス、回収、中古販売などの各ステージで判断し、評価するシステムが開示されている。

【0003】また、特開平11-120308号公報によると、製品機器に関する履歴情報を製品と一緒に記憶されるようにした履歴情報記憶装置が開示されている。

【0004】

【発明が解決しようとする課題】しかしながら、従来技術によると、製品に関する情報を製品に付加し、製品と情報をと一体として、ライフサイクルを構成する各ステージを流通させることができ、製造、メンテナンス、回収、中古販売などの各ステージで製品に関する情報を共有し自由に利用することができるものの、製品に付加された情報は誰でも利用できるので、各業者は、秘密の情報を製品に付加することができないという問題点がある。このため、製品と製品に関する情報をと一体として、ライフサイクルを流通させる技術が現実に普及しない原因の一つとなっている。

【0005】本発明は、上記の問題点を解決するために、情報記憶媒体又は非接触ICタグが付された物品が複数ステージを流達する場合において、ステージ毎の秘密の情報を記憶することができる情報記憶媒体及び非接触ICタグ、前記非接触ICタグに対してステージ毎に秘密に情報を読み書きすることができるアクセス装置、非接触ICタグとアクセス装置とから構成されるアクセスシステム、非接触ICタグとステージ毎に設けられるアクセス装置とを含むライフサイクル管理システム、非接触ICタグで用いられる入出力方法及びアクセス装置で用いられるアクセス方法を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明は、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な情報記憶媒体であって、複数の記憶領域を有する記憶手段と、各記憶領域を識別する識別子を格納している格納手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記格納手段に格納されている識別子のいずれかと一致するか否かを判断する判断手段と、一致すると判断される場合に、前記アクセス装置からアクセス情報を記憶する記憶手段と、記憶された情報を受信するアクセス情報受信手段と、受信したアクセス情報を基づいて、前記アクセス識別子により識別さ

れる記憶領域へのアクセスを行う入出力手段とを備える。

【0007】この構成によると、秘密に受信したアクセス識別子により識別される記憶領域に対して、アクセス装置はアクセスすることができるので、1個の情報記憶媒体を複数の目的において共用できるという効果がある。また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流達する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、前記したアクセス情報を基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行いう入出力手段とを備える。

【0008】この構成によると、秘密に受信したステージ識別子により識別されるステージ記憶領域に対して、アクセス装置はアクセスすることができるので、生産から廃棄に至るまでのライフサイクルにおける複数のステージにおいて、1個の非接触ICタグを、共用できるという効果がある。ここで、前記秘密受信手段は、第1認証子を生成し、生成した第1認証子を前記アクセス装置へ出力する認証子出力手段と、前記アクセス識別子を暗号化鍵として用いて、出力した前記第1認証子を暗号アルゴリズムが施されて生成された第2認証子を前記アクセス装置から取得する取得手段と、前記複数のステージ識別子を暗号化鍵として用いて、生成した前記第1認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第3認証子を生成する時号手段とを含み、前記判断手段は、取得した第2認証子が生成した複数の第3認証子のうちのいずれか1個と一致するか否かを判断し、一致する場合に、受信した前記アクセス識別子が前記識別子記憶手段に格納されているステージ識別子のいずれかと一致すると判断し、前記入出力手段は、前記アクセス識別子により識別されるステージ記憶領域として、前記第2認証子に一致する第3認証子を生成する際に暗号化鍵として用いたされたステージ識別子により識別されるステージ記憶領域へのアクセスを行うように構成してもよい。

【0009】この構成によると、非接触ICタグは、ステージ識別子を送信されることなく、アクセス装置を認証するので、ステージ識別子が外部に漏洩することがないという効果がある。ここで、前記認証子出力手段は、ラ

9
ンダムに第1認証子を生成するように構成してもよい。
【0010】この構成によると、非接触ICタグは、ランダムに認証子を生成するので、過去の通信により、ステージ識別子が外部に漏れることがないという効果がある。ここで、前記秘密受信手段は、時分割多重された通信チャネルのうち、1個の通信チャネルを選択手段と、選択された前記通信チャネルを介して、アクセス識別子を秘密に受信する識別子受信手段とを含むように構成してもよい。

【0011】この構成によると、非接触ICタグは、時分割多重された通信チャネルを用いて、アクセス装置と通信を行うので、アクセス装置は、同一時間帯において、複数の非接触ICタグと通信を行うことができるという効果がある。ここで、前記チャネル選択手段は、時分割多重された通信チャネルのうち、1個の通信チャネルを選択するように構成してもよい。

【0012】この構成によると、非接触ICタグは、ランダムに時分割された通信チャネルを選択するので、非接触ICタグ同士で通信チャネルが重なる可能性が少なくなるという効果がある。ここで、前記記憶手段は、さらに、共有識別子により識別される共有記憶領域を有し、前記識別子記憶手段は、さらに、前記共有識別子を記憶しており、前記判断手段は、さらに、受信した前記アクセス識別子が前記識別子記憶手段に記憶されている共有識別子と一致するか否かを判断し、前記アクセス情報受信手段は、さらに、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信し、前記出入力手段は、さらに、受信したアクセス情報に基づいて、前記アクセス識別子により識別される共有記憶領域へのアクセスを行うように構成してもよい。

【0013】この構成によると、非接触ICタグは、共有識別子により識別される共有領域を有しているので、複数のステージにおいて、同じ情報を共用できるという効果がある。ここで、非接触ICタグが有する不揮発性メモリは、ヒューズメモリであるとしてもよい。

【0014】この構成によると、データの改竄を防ぐことができる。本発明の非接触ICタグは、前記物品の表面に備えられたロゴタイプの傍に備えられるとしてもよい。これにより、非接触ICタグは外部から目立つことが無くなり、製品の外観を損なうことはない。また、情報記憶媒体の所在を統一することができ、ライフサイクルの各工程において、非接触ICタグの所在を明確にすることができます。

【0015】さらに、前記記憶手段にてデータを記憶する際に、併せて時刻情報を記憶する時刻情報記憶手段を備えるとしてもよい。これにより、物品情報をメモリに書き込むときにメモリが不足しても、物品情報が、年月日および時刻の情報を有しているので、最古の物品情報を自動で削除したり、リーダライタに物品情報のリストを送信し、リーダライタの使用者の応答により選択し

て物品情報を削除することで、新規の物品情報をメモリに書き込むことができる。

【0016】さらに、前記記憶手段は、データを上書きできない第1のメモリ部と、データを上書きできる第2のメモリ部とを有するとしてもよい。これにより、消去すべきでない、例えば製品のID情報などの基本情報は、消去できない第1のメモリ部に書き込んでおき、消去しても問題がない情報、あるいは一時的に書き込んだ情報は、消去可能な第2のメモリ部に使用者の必要性に応じて書き込むことができる。

【0017】さらに、前記記憶手段は、さらに、拡張記憶領域を有し、拡張記憶領域以外の記憶領域において空き容量不足によりデータを記憶できないときは、前記拡張記憶領域に記憶するとしてもよい。これにより、物品情報をメモリに書き込むときにメモリが不足しても、予め用意された拡張記憶領域に新規の物品情報を書き込むことができる。

【0018】また、前記記憶手段が空き容量不足によりデータを記憶できない場合、前記時刻情報がもっとも古いデータを削除して、空き容量を増加させる記憶整理手段を備えるとしてもよい。これにより、新たにデータをメモリに書き込むときに空き容量が不足しても、メモリに格納されたデータに添付された時刻情報を参照して最も古いデータを自動削除するので、新規データをメモリに書き込むことができる。

【0019】また、マスタ識別子を記憶するマスタ識別子記憶手段と、受信した前記アクセス識別子が前記マスタ識別子記憶手段に記憶されているマスタ識別子と一致するか否かを判断するマスタ識別子判断手段と、前記マスタ識別子判断手段が一致すると判断した場合に、前記アクセス装置からマスタアクセス情報を受信するマスタアクセス情報受信手段と、前記マスタアクセス情報をに基づいて、所定のステージ記憶領域へのアクセスを行う出入力手段と、更に、備えるとしてもよい。

【0020】これにより、非公開情報を強制的に公開させる必要が生じた場合、例えば非接触ICタグを付与された物品に不具合が生じ、その責任の所在を明らかにしなければならないような場合に、マスタ識別子を用いて情報の公開を促すことができる。また、本発明は、入院から退院に至るまでの病院の療養サイクルにおける複数のステージを経由する入院患者に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、前記療養サイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、一致す

ると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段とを備える。

【0021】この構成によると、各ステージのリーダライタを操作する権限を有する者、例えば、患者、医者、看護者又は会計担当者などは、自分が秘密に知っているパスワードをリーダライタに入力し、正しく権限を有する者である場合には、リーダライタは、無線I Cタグの各ステージ領域から情報を読み出し、又は情報を書き込む。これにより、患者は、自分の病状や治療方法について正しい知識を得ることができる。また、医者又は看護者が患者を取りえたり、処置を誤したりすることを防止ができる。また、会計担当者は、正確に治療代金などを計算できる。

【0022】また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流逝する高級ブランド品に付され、不揮発性メモリを有し、電波を用いて非接触で読み書き可能な非接触I Cタグであって、前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、一致するか否かを判断する場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段とを備える。

【0023】この構成によると、高級ブランド品の偽物の流布を防止することができる。また、高級ブランド品の品質を保証することができる。また、流通経路において、経路情報を無線I Cタグに書き込むことにより、流通の経路の管理、探索ができる。また、本発明は、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別される複数個の記憶領域を有し、電波を用いて非接触で読み書き可能な情報記憶媒体に対して情報を送受信するアクセス装置であって、アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記情報記憶媒体に対して送信する秘密送信手段と、前記情報記憶媒体により、秘密に送信した前記アクセス識別子が前記情報記憶媒体が有する複数個の記憶領域うちの1個の記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備える。

【0024】この構成によると、秘密に受信したアクセス識別子により識別される記憶領域を有する情報記憶媒

体に対して、アクセス装置はアクセスすることができるので、1個の情報記憶媒体を複数の目的において共用できることという効果がある。また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流逝する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触で読み書き可能な非接触I Cタグに対して情報を送受信するアクセス装置であって、アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子暗号を用いて秘密に前記非接触I Cタグに対して送信する秘密送信手段と、前記非接触I Cタグにより、秘密に送信した前記アクセス識別子が前記非接触I Cタグに有する複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備える。

【0025】この構成によると、秘密に受信したステージ識別子により識別されるステージ記憶領域を有する非接触I Cタグに対して、アクセス装置はアクセスするこ

とができるので、生産から廃棄に至るまでのライフサイクルにおける複数のステージにおいて、1個の非接触I Cタグを、共用できるという効果がある。ここで、前記非接触I Cタグは、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶しており、前記秘密送信手段は、前記非接触I Cタグから第1認証子を受信する認証子受信手段と、前記アクセス識別子を暗号化して用いて、受信した前記第1認証子に暗号アルゴリズムを施して第2認証子を生成し、生成した第2認証子を前記非接触I Cタグへ出力する認証子出力手段とを備え、前記アクセス情報送信手段は、前記非接触I Cタグにより、前記複数のステージ識別子を暗号化して用いて、前記第1認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第3認証子が生成され、出力された前記第2認証子が生成した複数の第3認証子のうちのいずれか1個と一致するか否かを判断され、一致する場合に、前記アクセス識別子が前記複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断されるときに、さらにアクセス情報を送信するように構成してもよい。

【0026】この構成によると、ステージ識別子を秘密に非接触I Cタグに対して送信することなく、非接触I Cタグにより認証されるので、ステージ識別子が外部に漏れることがないという効果がある。また、本発明に係るアクセス装置は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流逝する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触で読み書き可能な非接触I Cタグに対して情報を送受信

するアクセス装置であって、アクセス識別子を受け付ける識別子受付手段と、前記アクセス識別子を暗号を用いて秘密に前記非接触ICタグに対して送信する秘密送信手段と、前記非接触ICタグにより、秘密に送信した前記アクセス識別子が前記非接触ICタグが有する複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備えることを特徴とする。

【0027】これにより、ライフサイクルの各工程において同じ機能のリーダライタを用いても、各工程同士のセキュリティを図ることができる。また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成されライフサイクルを構成するステージ数と同数のステージ記憶領域を備え、電波を用いて非接触に読み書き可能な非接触ICタグと前記非接触ICタグに対して情報を送受信するアクセス装置とから構成されるアクセスシステムであって、前記非接触ICタグと、前記アクセス装置とから構成される。

【0028】この構成によると、上記に示す非接触ICタグ及びアクセス装置と同様の効果を奏することは明らかである。また、本発明は、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグが付された物品が、生産から廃棄に至るまでの複数ステージを流通する物品ライフサイクルにおいて、ステージ毎に設けられたアクセス装置により前記非接触ICタグにアクセスすることにより、前記物品を管理するライフサイクル管理システムであって、前記非接触ICタグと、前記アクセス装置とを含み、ステージ毎に設けられたアクセス装置により、前記非接触ICタグが有し、当該ステージに対応する1のステージ記憶領域のみアクセスすることにより、前記物品を管理する。

【0029】この構成によると、ステージ毎に設けられたアクセス装置により、前記非接触ICタグが有し、当該ステージに対応する1のステージ記憶領域のみアクセスすることにより、前記物品を管理するので、各ステージにおいて、上記に示す非接触ICタグ及びアクセス装置と同様の効果を奏することは明らかである。また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能であり、前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段とを備える非接触ICタグにより用いられる入出力方法であって、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信ステップと、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいず

れかと一致するか否かを判断する判断ステップと、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信ステップと、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力ステップとを含む。

【0030】この方法を用いると、前記非接触ICタグと同様の効果を奏することは明らかである。また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触ICタグにに対して情報を送受信し、アクセス識別子を記憶している識別子記憶手段を備えるアクセス装置により用いられるアクセス方法であって、前記アクセス識別子暗号を用いて秘密に前記非接触ICタグに対して送信する秘密送信ステップと、前記非接触ICタグにより、秘密に送信した前記アクセス識別子が前記非接触ICタグが有する複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信ステップとを含む。

【0031】この方法を用いると、前記アクセス装置と同様の効果を奏することは明らかである。

【0032】

【発明実施の形態】1 第1の実施の形態

本発明1の実施の形態としてのライフサイクル管理システム10について説明する。

30 1.1 製品のライフサイクル

生産者は、生産工場において、部品を加工し、組み立てて、製品(物品)を生産し、生産した製品を出荷する。物流業者は、出荷された製品を販売業者へ輸送する。販売業者は、製品を需要者に販売し、需要者は、その製品を使用する。サービス業者は、需要者により使用されている製品を補修・修理する。回収リサイクル業者は、長年使用された製品を解体、廃棄する。解体された製品の一部は、再度製品を加工する際に部品として使用される。

40 【0033】こうして、製品は、図1に示すように、生産1、物流2、販売3、サービス4、回収リサイクル5の各ステージを経て流通し、その一生を終える。製品の生産から廃棄・回収に至るまでを、製品のライフサイクル6と呼ぶ。生産業者は、その生産の1工程において、1個の無線ICタグ(後述する)を製品に付す。例えば、テレビ受像機の生産業者は、図2に示すように、テレビ受像機8の前面枠部分8'1に、無線ICタグ8'0aを貼り付け、貼り付けた無線ICタグ8'0aの上面に、ロゴマーク8'3を貼り付ける。また、衣服の生産業者は、図3に示すように、ラベル9'3の裏面に無線IC

タグ80 bを貼り付け、無線ICタグ80 bを貼り付けたラベル93を衣服90の襟裏側部91に縫い付ける。

【0034】無線ICタグは、前記製品に関する情報を記憶する領域を備えている。生産業者は、生産の工程において、無線ICタグに生産に関する情報を書き込み、又は無線ICタグから参照することにより、製品の生産管理を行う。物流業者は、製品の輸送の過程において、無線ICタグに輸送に関する情報を書き込み、又は無線ICタグから参照することにより、製品の輸送管理を行う。同様にして、販売業者、サービス業者及び回収リサイクル業者は、それぞれの業務のプロセスにおいて、無線ICタグにそれぞれの業務に関する情報を書き込み、又は無線ICタグから参照することにより、製品の業務管理を行う。

【0035】このように、複数のステージにおいて、製品に付された1個の無線ICタグに対して、情報の書き込みと参照とが行われる。

1.2 ライフサイクル管理システム10の構成
ライフサイクル管理システム10は、図4に示すように、生産管理サブシステム20 a、物流管理サブシステム20 b、販売管理サブシステム20 c、サービス管理サブシステム20 d、回収リサイクル管理サブシステム20 e及びインターネット30から構成されている。各サブシステムは、インターネット30を介して相互に接続されている。

【0036】生産管理サブシステム20 a、物流管理サブシステム20 b、販売管理サブシステム20 c、サービス管理サブシステム20 d及び回収リサイクル管理サブシステム20 eは、それぞれ、前記生産業者、前記物流業者、前記販売業者、前記サービス業者及び前記回収リサイクル業者による製品の管理を行うための情報管理システムである。

1.3 サブシステム20の構成
生産管理サブシステム20 a、物流管理サブシステム20 b、販売管理サブシステム20 c、サービス管理サブシステム20 d及び回収リサイクル管理サブシステム20 eは、共通の構成を有している。これらのサブシステムをサブシステム20として、以下において説明する。

【0037】(1) サブシステム20の構成
サブシステム20は、図5に示すように、商品に貼り付けられた無線ICタグ80とリーダライタ30 a(30 b)と管理装置40 a(40 b)とからなる第1組、携帯電話型リーダライタ30 cと基地局50と受信装置51と接続装置53とからなる第2組、リーダライタ30 dと携帯電話内蔵型管理装置40 dと基地局50と受信装置51と接続装置53とからなる第3組、携帯端末型リーダライタ30 eとICカード52と管理装置40 eとからなる第4組、データベース61を有するホストコンピュータ60及びLAN装置70から構成される。

【0038】第1組において、リーダライタ30 a(3

0 b)は管理装置40 a(40 b)に接続され、管理装置40 a(40 b)はLAN装置70に接続されている。第2組において、携帯電話型リーダライタ30 cは、基地局50及び公衆回線網を介して、受信装置51と通信を行い、受信装置51は接続装置53に接続され、接続装置53はLAN装置70に接続されている。

【0039】第3組において、リーダライタ30 dは、携帯電話内蔵型管理装置40 dに接続され、携帯電話内蔵型管理装置40 dは、基地局50及び公衆回線網を介して、受信装置51と通信を行い、受信装置51は接続装置53に接続され、接続装置53はLAN装置70に接続されている。第4組において、ICカード52は携帯端末型リーダライタ30 e又は管理装置40 eに装着される。携帯端末型リーダライタ30 eはICカード52にデータを書込み、又はICカード52からデータを参照する。また、管理装置40 eはICカード52にデータを書込み、又はICカード52からデータを参照する。管理装置40 eは、LAN装置70に接続されている。

20 【0040】ホストコンピュータ60は、LAN装置70に接続されている。また、LAN装置70は、インターネット30に接続されている。

(2) 第1組のリーダライタ30 a及び管理装置40 a 生産管理サブシステム20 aに含まれる第1組のリーダライタ30 a及び管理装置40 aが、生産工場内に設置されている状況を、図6に示す。この図に示すように、生産工場内において、無線ICタグが張り付けられたテレビ受像機が段ボール箱内に梱包され、テレビ受像機の梱包された段ボール箱がベルトコンベア上を移動している。この図に示すように、管理装置40 aは、所謂パーソナルコンピュータと同様に、ディスプレイ部と本体部とキーボード部とから構成されている。また、リーダライタ30 aは、円筒形状を有する本体部と本体部上端に備えられたアンテナ部から構成され、アンテナ部と、リーダライタ30 aの近辺のベルトコンベア上を移動する段ボール箱との間ににおいて、アンテナ部から送信される電波を遮る物がないように、ベルトコンベアに近接して設置されている。

【0041】(3) 第3組のリーダライタ30 d及び携帯電話内蔵型管理装置40 d 物流管理サブシステム20 bに含まれる第3組のリーダライタ30 d及び携帯電話内蔵型管理装置40 dが、貨物トラックに搭載されている様子を、図7に示す。この図に示すように、携帯電話内蔵型管理装置40 dは、所謂ノートブック型パーソナルコンピュータと同様に、液晶ディスプレイ部とキーボードを兼ねた本体部と基地局50と間で電波の送受信を行うアンテナ部とから構成され、貨物トラックの助手席前方に設置されている。また、リーダライタ30 dは、アンテナ部を有し、貨物トラックの荷物搬入口の上部内側において、アンテナ部か

ら下向に電波が送信されるように、取り付けられている。

【0042】(4) 第2組の携帯電話型リーダライタ30c

物流管理サブシステム20bに含まれる第2組の携帯電話型リーダライタ30cの外観を図8に示す。携帯電話型リーダライタ30cは、所謂携帯電話と同様の形状を有する本体部からなり、本体部の前端側面において、基板50と間で電波を送受信するアンテナ部と備え、本体部の操作側面において、複数の操作ボタンと表示部とマイクとスピーカとを備えている。

【0043】(5) 第1組のリーダライタ30b

販売管理サブシステム20cに含まれる第1組のリーダライタ30bの外観を図9に示す。リーダライタ30bは、円筒形状の本体部を有し、本体部の前端側面に無線ICタグとの間で電波を送受信するアンテナ部を備え、本体部側面に操作ボタンを備えている。第1組のリーダライタ30bは、同一時間帯において、複数の無線ICタグとの間でデータの読み書きを行う。

【0044】(6) 第4組の携帯端末型リーダライタ30e

サービス管理サブシステム20dに含まれる第4組の携帯端末型リーダライタ30eの外観を図10に示す。携帯端末型リーダライタ30eは、本体部の前端側面において、無線ICタグとの間で電波を送受信するアンテナ部とプリント部とを備え、本体部側面において、複数の操作ボタンと表示部と備え、本体部の後端側面において、ICカード挿入口を備えており、ICカード挿入口には、ICカードF52が装着される。また、管理装置40eには、所謂パーソナルコンピュータと同様に、ディスプレイ部と本体部とキーボード部とを含み、さらにICカード入出力部を備えており、ICカード入出力部には、ICカードF52が装着される。

1.4 リーダライタ30の構成

リーダライタ30a、30b及び30dは、同様の構成を有する。また、携帯電話型リーダライタ30c、携帯端末型リーダライタ30eは、リーダライタ30aと同様の構成を内蔵する。ここでは、これらの装置をリーダライタ30として説明する。

【0045】リーダライタ30は、同一時間帯において、最大50個の無線ICタグに対して情報の読み書きができる。リーダライタ30は、図11に示すように、入出力部101、制御部102、一時記憶部103、命令生成部104、クロック生成部105、識別コード記憶部106、録記憶部107、暗号化部108、ハシユ部109、命令解読部110、変復調部111及びアンテナ部112から構成される。

【0046】(1) 一時記憶部103

一時記憶部103は、無線ICタグを識別する50個の

識別コードをそれぞれ一時的に記憶する50個の識別コード領域を有する。

(2) 識別コード記憶部106

識別コード記憶部106は、それぞれ50個の識別コードを記憶する領域を有する。

【0047】(3) 録記憶部107

録記憶部107は、リーダライタ30に許可されている無線ICタグの後述するステージ領域の1個をアクセスするための領域鍵K1と、無線ICタグの後述する共通領域をアクセスするための領域鍵K2とを記憶している。これらの領域鍵は、56ビット長である。

【0048】なお、リーダライタ30に許可されている無線ICタグのステージ領域が、前記1個のステージ領域以外のステージ領域である場合には、そのステージ領域に応じて、領域鍵K1の代わりに、領域鍵K2～K5のいずれか1個を記憶している。領域鍵K2～K5は、それぞれ6ビット長である。

(4) 入出力部101

入出力部101は、後述する管理装置40と接続されており、管理装置40から入出力命令と入出力情報とからなる組を受け取る。

【0049】入出力命令は、入力命令又は出力命令からなる。入力命令は、無線ICタグが有するメモリからデータを読み出す命令であり、出力命令は、無線ICタグが有するメモリにデータを書き込む命令である。入出力命令が入力命令である場合に、入出力情報は、無線ICタグのメモリの物理アドレスと読み出しバイト数とを含む。入出力命令が出力命令である場合に、入出力情報は、無線ICタグのメモリの物理アドレスと書き込みバイト数と書き込み内容とを含む。

【0050】入出力部101は、受け取った入出力命令と入出力情報を制御部102へ出力する。また、制御部102からアクセス応答命令とアクセス応答情報と識別コードとを受け取り、管理装置40へ受け取ったアクセス応答命令とアクセス応答情報と識別コードとを出力する。

(5) 制御部102

制御部102は、図12に示すように、充電電波送信期間、同期信号送信期間、識別コード収集期間及びアクセス期間において、それぞれ、充電電波送信の制御、同期信号送信の制御、識別コード収集の制御及びアクセスの制御を行う。この図において、横軸は時間軸である。

【0051】充電電波送信期間、同期信号送信期間、識別コード収集期間及びアクセス期間は、この順序で時間軸上で隣接している。識別コード収集期間は、第1収集期間と第2収集期間とからなり、第1収集期間と第2収集期間とは、それぞれ、識別コード送信期間、識別コード応答期間及び識別コード一致期間から構成される。識別コード送信期間、識別コード応答期間及び識別コード一致期間は、それぞれ、500m秒長の一周期を形成す

る。

【0052】1周期は、50個の10m秒長に均等に分割される。各10m秒長を、チャネルと呼ぶ。1周期内の50個のチャネルを、1周期の先頭から順にそれぞれチャネル1、チャネル2、チャネル3、・・・、チャネル50と呼び、50個のチャネルは、これらのチャネル番号により識別される。

(命令の出力)制御部102は、入出力部101から、入出力命令と入出力情報とを受け取る。入出力命令を受け取ると、命令生成部104に対して、同期信号を送信する旨の同期信号送信命令及び各無線ICタグの識別コードを収集する旨の識別コード収集命令をこの順序で出力する。

【0053】(識別コードの収集)制御部102は、命令生成部104に対して、識別コード収集命令を出力した後、3秒間の識別コード収集期間において、次に示すようにして、各無線ICタグから識別コードを収集する。前記識別コード収集期間が経過する、制御部102は、各無線ICタグから識別コードの収集が終了したとみなし、識別コードの収集を終了する。識別コード収集期間は、上記に説明したように、第1収集期間と第2収集期間とに分かれしており、第1収集期間と第2収集期間とのそれそれにおいて、制御部102は、識別コード送信の制御、識別コード応答の制御、識別コード一致の制御を行う。このように、第1収集期間と第2収集期間とのそれそれにおいて、2回の収集を行う理由については、後述する。

【0054】制御部102は、識別コード送信期間において、命令解読部110から識別コード送信命令と識別コードとを受け取り、ハッシュ部109からハッシュ値を受け取る。識別コード送信命令を受け取ると、受け取った識別コードを、一時記憶部103内の前記受け取ったハッシュ値により示される識別コード領域へ書き込む。

【0055】制御部102は、クロック生成部105から基準クロックを受け取り、受け取った基準クロックに基づいて、10m秒間に1個のパルス信号からなる同期信号を繰り返し含む同期信号波を生成し、生成した同期信号波を100m秒間、命令生成部104へ出力する。図12に示すように、同期信号波の1周期は、5000m秒であり、前述したように、1周期は、50個の10m秒長に均等に分割され、各10m秒長を、チャネルと呼ぶ。

【0056】制御部102は、受け取ったハッシュ値をチャネル番号とするチャネルを選択し、識別コード応答期間内の、選択したチャネルにおいて、前記受け取った識別コードと、前記識別コードを送信する旨を示す識別コード応答命令とを命令生成部104へ出力する。このように、制御部102は、受け取ったハッシュ値をチャネル番号としてチャネルを選択するので、異なる無線ICタグに対して同じチャネルが選択される可能性がある。この場合において、これらの無線ICタグについては、第1収集期間における識別コードの収集は諦め、第2収集期間において、これらの無線ICタグの識別コードの収集を行いう。この第2収集期間において、これらの異なる無線ICタグに対して同じチャネルが選択される可能性は低くなる。

【0057】制御部102は、識別コード一致期間内の選択したチャネルにおいて、命令解読部110から識別コード一致命令の受け取りを待ち受ける。選択したチャネルにおいて、命令解読部110から識別コード一致命令を受け取ると、前記一時記憶部103の前記ハッシュ値により示される識別コード領域に記憶されている識別コードが正しく前記無線ICタグを識別する識別コードであると認識し、前記一時記憶部103に記憶されている前記識別コード読み出し、読み出した識別コードを識別コード記憶部108へ書き込む。

(無線ICタグからの認証と領域アクセス)制御部102は、識別コード記憶部106に記憶されている全ての識別コードについて、以下に示すように、アクセス期間において、各識別コードにより識別される無線ICタグへのアクセス要求と無線ICタグの領域アクセスを行いう。

【0058】制御部102は、アクセス期間において、識別コード記憶部106から1個の識別コードを読み出し、読み出した識別コードにより識別される無線ICタグに対するアクセスを要求する旨のアクセス要求命令と、前記読み出した識別コードとを命令生成部104へ出力する。制御部102は、命令解読部110から認証子送信命令と識別コードとを受け取る。認証子送信命令を受け取ると、鍵記憶部107に記憶されている領域鍵(K1又はK6)を読み出し、読み出した領域鍵(K1又はK6)を暗号化部108へ出力する。読み出す領域鍵がK1であるか又はK6であるかは、入出力部101から受け取る入出力情報により決定する。入出力情報に含まれる物理アドレスが、リーダライタ30に許可されている無線ICタグのステージ領域内を示す場合には、K1を読み出す。入出力情報に含まれる物理アドレスが、リーダライタ30の共通領域内を示す場合には、K6を読み出す。

【0059】制御部102は、命令生成部104へ前記読み出した識別コードと認証子応答命令とを出力する。制御部102は、命令解読部110からアクセス不許可命令と識別コードと理由コードとを受け取る。アクセス不許可命令と識別コードと理由コードとを受け取ると、受け取った理由コードに基づいて、領域鍵K1の誤り等操作の誤りであると認識し、識別コードで識別される無線ICタグへのアクセスを諦める。次にアクセス応答命令を生成し、理由コードを含むアクセス応答情報を生成し、アクセス応答命令とアクセス応答情報と識別コード

21
とを入出力部101へ出力する。

【0060】制御部102は、入出力命令に基づいてアクセス命令を生成し、入出力情報に基づいてアクセス情報を生成し、命令生成部104へ、前記読み出した識別コードとアクセス情報とアクセス命令とを出力する。制御部102は、命令解読部110から、アクセス応答命令とアクセス応答情報と識別コードとを受け取り、受け取ったアクセス応答命令とアクセス応答情報と識別コードとを入出力部101へ出力する。

【0061】なお、各命令は、4ビット長からなるコードである。制御部102は、無線ICタグから放射される電波を受信する期間内において、変復調部111に対して、無信号波を出力するように、制御する。この期間とは、識別コード送信期間、識別コード一致期間、アクセス期間であり、無線ICタグからデータを受信する期間である。

【0062】(6) 命令生成部104

命令生成部104は、制御部102から、同期信号送信命令、識別コード収集命令、識別コードと識別コード応答命令との組、アクセス要求命令と識別コードとの組、識別コードと認証子応答命令との組、及び識別コードとアクセス情報とアクセス命令との組を受け取る。

【0063】これらの命令と命令に付随するオペランド等を図13に示す。命令生成部104は、制御部102から同期信号送信命令を受け取ると、受け取った同期信号送信命令に基づいて、パルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。続いて、制御部102から同期信号波を受け取り、受け取った同期信号波に基づいて、パルス信号波を1秒間生成し、生成したパルス信号波を変復調部111へ出力する。

【0064】命令生成部104は、制御部102から識別コード収集命令、識別コード応答命令、アクセス要求命令、認証子応答命令又はアクセス命令を受け取ると、それぞれの命令に基づいて、パルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。命令生成部104は、制御部102から識別コードと識別コード応答命令とを受け取ると、識別コード応答命令に基づくパルス信号波の出力に引き続いで、受け取った識別コードに基づいてパルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。

【0065】命令生成部104は、制御部102からアクセス要求命令と識別コードとを受け取ると、アクセス要求命令に基づくパルス信号波の出力に引き続いで、受け取った識別コードに基づいてパルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。命令生成部104は、制御部102から識別コードと認証子応答命令とを受け取り、暗号化部108から暗号化乱数R'0を受け取ると、認証子応答命令に基づくパルス信号波の出力に引き続いで、受け取った識別コードと暗号化乱数R'0'に基づいてパルス信号波を生成し、生

成したパルス信号波を変復調部111へ出力する。

【0066】命令生成部104は、制御部102から識別コードとアクセス情報とアクセス命令とを受け取ると、アクセス命令に基づくパルス信号波の出力に引き続いで、受け取った識別コードとアクセス情報とに基づいてパルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。

(7) クロック生成部105

クロック生成部105は、基準時刻を示す基準クロックを繰り返し生成し、生成した基準クロックを制御部102へ出力する。

【0067】(8) 暗号化部108

暗号化部108は、暗号アルゴリズムE1を備えている。ここで、暗号アルゴリズムE1は、DES（データ暗号化規格、Data Encryption Standard）により規定されている暗号アルゴリズムである。この暗号アルゴリズムの暗号鍵は56ビット長であり、この暗号アルゴリズムE1に入力される平文及びこの暗号アルゴリズムE1により生成される暗号文の長さは64ビットである。

【0068】暗号化部108は、制御部102から領域鍵(K1又はK6)を受け取り、命令解読部110から乱数R0を受け取り、領域鍵(K1又はK6)を用いて、受け取った乱数R0に暗号アルゴリズムE1を施して、暗号化乱数R'0'を生成し、生成した暗号化乱数R'0'を命令生成部104へ出力する。なお、この明細書において、鍵Kを用いて、平文Mに対して、暗号アルゴリズムEを施し、暗号文M'を生成するとき、次の式で示すように表現することとする。

【0069】C = E (M, K)

30 (9) ハッシュ部109

ハッシュ部109は、命令解読部110から乱数R0を受け取り、受け取った乱数R0を入力値として、ハッシュ関数Hを施して、ハッシュ値を生成する。生成されるハッシュ値は、1～50の50個の値のうちのいすれかの1個の値となる。前記ハッシュ関数Hは、入力値に基づいて、入力値を前記50個の値に均等に振り分け、入力値が振り分けられた1個の値をハッシュ値として生成する。

【0070】ハッシュ部109は、生成したハッシュ値を制御部102へ出力する。

(10) 命令解読部110

命令解読部110は、変復調部111からパルス信号波を受け取る。受け取ったパルス信号波を解読して、命令とオペランドとを抽出し、抽出した命令を制御部102へ出力する。抽出する命令には、図14に示すように、識別コード送信命令、識別コード一致命令、認証子送信命令、アクセス不許可命令及びアクセス応答命令が含まれる。これらの命令は、4ビット長からなる命令である。

50 【0071】命令解読部110は、抽出した命令が識別

コード送信命令である場合に、オペランドとして、乱数R0と識別コードとを抽出し、抽出した乱数R0をハッシュ部109へ出し、抽出した識別コードを制御部102へ出力する。命令解読部110は、抽出した命令が認証子送信命令である場合に、オペランドとして、乱数R0と識別コードとを抽出する。ここで、乱数R0は、リーダライタのステージ領域を認証するための認証子である。抽出した乱数R0を暗号化部108へ出し、抽出した識別コードを制御部102へ出力する。

【0072】命令解読部110は、抽出した命令が識別コード一致命令である場合に、オペランドとして、識別コードを抽出し、抽出した識別コードを制御部102へ出力する。命令解読部110は、抽出した命令がアクセス不許可命令である場合に、オペランドとして、識別コードと理由コードとを抽出し、抽出した識別コードと理由コードとを制御部102へ出力する。

【0073】命令解読部110は、抽出した命令がアクセス応答命令である場合に、オペランドとして、アクセス応答情報と識別コードとを抽出し、抽出したアクセス応答情報と識別コードとを制御部102へ出力する。

(11) 変復調部111

変復調部111は、命令生成部104からパルス信号波又は無信号波を受け取る。また、制御部102から無信号波を受け取る。パルス信号波を受け取ると、受け取ったパルス信号波を変調信号として、変調信号に基づいて2.45GHzの搬送波の振幅を変化させ、振幅の変化した搬送波をアンテナ部112へ出力する。また、無信号波を受け取ると、2.45GHzの搬送波をそのまま、アンテナ部112へ出力する。

【0074】また、変復調部111は、アンテナ部112から電力信号を受け取り、受け取った電力信号から2.45GHzの周波数を有する信号を選択し、選択した信号からパルス信号波を抽出し、抽出したパルス信号波を命令解読部110へ出力する。

(12) アンテナ部112

アンテナ部112は、送信アンテナと受信アンテナどちら構成される。

【0075】アンテナ部112は、送信アンテナとして、特定の方向に電波を放射する指向性アンテナである。変復調部111から振幅の変化した、又は変換していない搬送波を受け取り、電波として空間に放射する。アンテナ部112は、受信アンテナとして、電波を受信し、受信した電波を電力信号に変換して、電力信号を変復調部111へ出力する。

1.5 無線ICタグ80の構成

無線ICタグ80は、図15に示すように、長さ30mm、幅5mm、厚さ0.5mmの板状に成形された樹脂内に、ICチップ部200とアンテナ部201とが、封入されて形成されている。

【0076】なお、無線ICタグの形成方法について

は、特開平8-276458号公報に記載されているので、詳細の説明を省略する。無線ICタグ80の通信可能な距離は、1m程度以内であり、通信速度は、1.0～20m秒/byteである。また、無線ICタグ80は、50枚以内の重ね読み（マルチ読み）が可能である。

【0077】ICチップ部200は、図16に示すように、電源部203、復調部206、命令解読部207、識別コード記憶部208、制御部209、認証部210、乱数生成部211、ハッシュ部212、変調部213、クロック生成部214、入出力部215及びメモリ部216から構成される。ICチップ部200の寸法は、縦1mm、横1mm、厚さ0.25ミクロンである。

【0078】(1) 識別コード記憶部208

識別コード記憶部208は、無線ICタグ80を個別に識別する識別コードを記憶している。識別コードは、32ビットからなり、無線ICタグを製造する製造業者を識別する製造業者識別コード（10ビット長）と、無線ICタグが複数の仕様や種類を有する場合に、その仕様や種類などを識別する種類コード（10ビット長）と、製造業者及び種類毎に個別化異なる値が設定される製造番号（12ビット長）とから構成される。

【0079】(2) メモリ部216

メモリ部216は、1Kバイトの記憶容量を有するEEPROM（Electric Erasable and Programmable ROM）から構成される。なお、EEPROMに代えて、ヒューズROMを用いるとしてもよい。ヒューズROMは、一度データを書き込むと消去することができないタイプのメモリである。ヒューズROMを用いることにより、データの改竄を防ぐことができる。また、EEPROM及びヒューズROMの両方を用いるとしてもよい。

【0080】メモリ部216は、図17に示すように、非プロジェクト部301とプロジェクト部302とから構成され、非プロジェクト部301は、アドレス0～249（10進表示、以下同様にアドレスは10進表示。）に配置され、250バイトからなり、プロジェクト部302は、アドレス250～999に配置され、750バイトからなる。

【0081】非プロジェクト部301は、50バイトずつ5個の領域311～315から構成され、領域311～315は、それぞれ、アドレス0～49、50～99、100～149、150～199、200～249に配置されている。プロジェクト部302は、150バイトずつ5個の領域321～325から構成され、領域321～325は、それぞれ、アドレス250～399、400～549、550～699、700～849、850～999に配置されている。

【0082】領域311及び領域321、領域312及び領域322、領域313及び領域323、領域314

及び領域324、領域315及び領域325は、それぞれ5個の生産ステージ、物流ステージ、販売ステージ、サービスステージ、回収リサイクルステージのために用いられるステージ領域である。領域311～315は、領域K6によるアクセスが許可される共通領域である。領域321～325は、それぞれ領域K1～K5のみによるアクセスが許可される領域である。

【0083】ここで、領域K6によりこれらの共通領域へのアクセスが許可されているのは、領域K6を知る者へのみアクセスを許可することにより、不用意にデータの読み書きがされないようにするためである。領域321～325は、それぞれ1度だけ書き込みを行うライトワنس(WriteOnce)部と更新が可能な可変部とからなる。

【0084】各領域に情報が記録されているメモリ部216の一例を図18に示す。この図において、メモリ部216の内容をステージ領域毎に示している。生産ステージ領域には、非プロテクト部において、「メーカー名」、「品名」及び「品番」が記録され、プロテクト部のライトワنس部において、「製番」、「製造日」及び「工場名」が記録されている。

【0085】物流ステージ領域には、非プロテクト部において、「運送業者名」が記録され、プロテクト部のライトワنس部において、「入出庫日」及び「グローバルケーション番号(GLN)」が記録されている。販売ステージ領域には、非プロテクト部において、「保証期間」及び「保証番号」が記録され、プロテクト部のライトワنس部において、「卸業者名」、「小売店名」及び「販売日」が記録されている。

【0086】サービスステージ領域には、非プロテクト部において、「洗濯方法」が記録され、プロテクト部の可変部において、「修理者名」、「修理日」及び「修理部品」が記録されている。回収リサイクルステージ領域には、プロテクト部のライトワنس部において、「回収業者名」、「回収日」、「廃棄業者」及び「廃棄日」が記録され、プロテクト部の可変部において、「リユース記録」が記録されている。

【0087】(3) 電源部203

電源部203は、アンテナ部201と接続され、アンテナ部201から電力信号を受け取り、受け取った電力信号を電荷として蓄積する。また、無線ICタグ80の各構成部に電力を供給する。電源部203に含まれる電源回路の一例を、図19に示す。図19に示す電源回路は、4個のダイオードD1～D4と、電池Eから構成される。ダイオードD1～D2は、同じ方向に直列に接続され、ダイオードD3～D4は、同じ方向に並列に接続され、また、ダイオードD1～D2とダイオードD3～D4とは、同じ方向に並列に接続されている。アンテナ部201の一端は、ダイオードD1とD2との中间点に接続され、アンテナ部201の他の一端は、ダイオ

F D3とD4との中间点に接続されている。電池Eの一端は、ダイオードD1とD3との中间点に接続され、電池Eの他の一端はダイオードD2とD4との中间点に接続されている。

【0088】(4) 復調部206
復調部206は、インピーダンス切換部205から電力信号を受け取り、受け取った電力信号から2.45GHzの周波数を有する信号を選択し、選択した信号からパルス信号波を抽出し、抽出したパルス信号波を命令解読部207へ出力する。

【0089】(5) 命令解読部207
命令解読部207は、復調部206からパルス信号波を受け取る。受け取ったパルス信号波を解読して、命令とオペラントを抽出し、抽出した命令とオペラントを制御部209へ出力する。抽出する命令には、図13に示すように、同期信号送信命令、識別コード收集命令、アクセス要求命令、アクセス命令、識別コード応答命令及び認証子応答命令が含まれる。なお、これらの命令及びオペラントについては、前述したとおりであるので、説明は省略する。

【0090】(6) 制御部209
制御部209は、命令解読部207から命令とオペラントを受け取る。これらの命令には、同期信号送信命令、識別コード收集命令、アクセス要求命令、アクセス命令、識別コード応答命令及び認証子応答命令が含まれる。また、比較器235から、ステージ領域を識別する番号Xi(後述する)又は暗号化乱数が一致しない旨を受け取る。

【0091】制御部209は、同期信号送信命令を受け取ると、引き続き復調部206から同期信号波を受信し、受信した同期信号波に含まれる同期信号を抽出し、クロック生成部214から基準クロックを受け取り、受け取った基準クロックに基づいて、抽出した同期信号に同期する同期信号を繰り返し含む同期信号波を生成する。

【0092】(識別コードの出力) 制御部209は、識別コード收集命令を受け取ると、乱数生成部211に対して乱数を生成するよう指示する。次に、乱数生成部211から生成された乱数R0を受け取り、ハッシュ部212から生成されたハッシュ値を受け取り、識別コード記憶部から識別コードを読み出す。次に、制御部209は、受け取ったハッシュ値をチャネル番号とするチャネルを選択し、識別コード送信期間において、選択したチャネルにより、読み出した識別コードと乱数R0と識別コード送信命令とを変調部213へ出力する。

【0093】制御部209は、識別コード応答期間において、選択したチャネルにより、識別コード応答命令を受け取ると、さらに識別コードを受け取り、前記識別コード記憶部208から読み出した識別コードと、受け取った識別コードとを比較する。一致しているなら、識別

コード一致期間において、選択したチャネルにより、識別コードと識別コード一致命令とを変調部213へ出力する。一致していないなら、上記の乱数生成部211に対する乱数生成から再度繰り返す。

【0094】(アクセスの認証)制御部209は、アクセス期間において、アクセス要求命令を受け取ると、さらに識別コードを受け取る。次に、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較する。一致しなければ、さらに、アクセス要求命令の受け取りを待ち受ける。一致すれば、乱数生成部211に対して乱数を生成するように指示し、乱数生成部211から乱数R0を受け取り、識別コードと乱数R0と認証子送信命令とを変調部213へ出力する。

【0095】制御部209は、認証子応答命令を受け取ると、さらに、識別コードと暗号化乱数R0'を受け取る。次に、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較する。一致しなければ、さらに、認証子応答命令の受け取りを待ち受ける。一致すれば、暗号化乱数R0'を認証部210の比較器235へ出力する。

【0096】制御部209は、比較器235から暗号化乱数が一致しない旨を受け取ると、識別コードとアクセス不許可命令と理由コードとを変調部213へ出力する。ここで、理由コードは、許可されていないステージ領域のアクセスであることを示す。また、番号Xiを受け取ると、次にアクセス命令を受け取る。制御部209は、アクセス命令を受け取ると、さらに、識別コードとアクセス情報をとを受け取る。アクセス命令は、Read命令及びWrite命令からなる。アクセス命令がRead命令である場合には、アクセス情報は、物理アドレスと読み出したバイト数とを含み、アクセス命令がWrite命令である場合には、アクセス情報は、物理アドレスと書き込みバイト数と書き込み内容とを含む。次に、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較する。

【0097】一致しなければ、さらに、アクセス命令の受け取りを待ち受ける。一致すれば、アクセス情報に含まれる物理アドレスが番号Xiで示されるステージ領域内を示しているか否かを判断し、ステージ領域内を示していない場合には、識別コードとアクセス不許可命令と理由コードとを変調部213へ出力する。ここで、理由コードは、許可されていないステージ領域のアクセスであることを示す。ステージ領域内を示している場合には、受け取ったアクセス命令とアクセス情報をとを出入力部215へ出力する。

【0098】制御部209は、出入力部215から、メモリ部216から読み出した情報又は書き込み終了の情報を受け取る。前記読み出した情報又は書き込み終了の情報を受け取ると、識別コードとアクセス応答命令とアクセス応答情報をとを変調部213へ出力する。ここで、ア

セス応答情報は、メモリ部216から読み出した情報又は書き込み終了の情報である。

【0099】(7)認証部210

認証部210は、図20に示すように、鍵記憶部231と乱数記憶部232と暗号化部233と生成乱数記憶部234と比較器235とを備えている。

(a) 鍵記憶部231

鍵記憶部231は、無線ICタグ80の5個のステージ領域をそれぞれアクセスするための領域鍵K1～K5と、共通領域をアクセスするための領域鍵K6とを記憶している。これらの領域鍵は、それぞれ56ビット長である。

【0100】(b)乱数記憶部232

乱数記憶部232は、乱数生成部211から乱数R0を受け取り、受け取った乱数R0を記憶する。

(c) 暗号化部233

暗号化部233は、暗号化部108が備える暗号アルゴリズムE1と同じ暗号アルゴリズムE1を備えている。

【0101】暗号化部108は、鍵記憶部231から領

域鍵K1～K6を読み出し、乱数記憶部232から乱数R0を読み出し、読み出した領域鍵K1～K6を用いて、読み出した乱数R0に暗号アルゴリズムE1を施して、それぞれ暗号化乱数R1～R6を生成し、生成した暗号化乱数R1～R6を生成乱数記憶部234に書き込む。

【0102】(d)生成乱数記憶部234

生成乱数記憶部234は、暗号化乱数R1～R6を記憶する。

(e) 比較器235

30 比較器235は、命令解读部207から暗号化乱数R0'を受け取り、受け取った暗号化乱数R0'に一致する暗号化乱数を生成乱数記憶部234から探し、一致する暗号化乱数があれば、一致する暗号化乱数を識別する番号Xiを制御部209へ出力する。例えば、一致する暗号化乱数がR1であれば、番号Xiは、1であり、一致する暗号化乱数がR2であれば、番号Xiは、2である。この番号Xiは、ステージ領域を識別する番号である。番号Xiが1～5の場合、それぞれ、生産用、物流用、販売用、サービス用、回収リサイクル用のステージ領域を識別する。

【0103】一致する暗号化乱数がなければ、暗号化乱数が一致しない旨を制御部209へ出力する。

(8)乱数生成部211

乱数生成部211は、制御部209から乱数生成の指示を受け取る。前記指示を受け取ると、乱数R0を生成する。乱数R0は、160ビット長である。生成した乱数R0をハッシュ部212と認証部210と制御部209とへ出力する。

【0104】(9)ハッシュ部212

50 ハッシュ部212は、乱数生成部211から乱数R0を

受け取り、受け取った乱数R0を入力値として、ハッシュ関数Hを施して、ハッシュ値を生成する。ここで、ハッシュ関数Hは、ハッシュ部209が有するハッシュ関数と同じ関数である。生成されるハッシュ値は、1～50の50個の値のうちのいずれかの1個の値をとる。ハッシュ関数Hは、入力値に基づいて、入力値を前記50個の値に均等に振り分け、入力値が振り分けられた1個の値をハッシュ値として生成する。

【0105】ハッシュ部212は、生成したハッシュ値を制御部209へ出力する。

(10) 変調部213

変調部213は、制御部402から命令とオペランドを受け取り、命令とオペランドとからなるビット列を生成し、生成したビット列に含まれるビット(0又は1)に応じて、アンテナ部201が有するインピーダンスを切り換える。具体的には、各ビットが「1」のとき、前記インピーダンスを第1の値とし、各ビットが「0」のとき、第2の値とする。これにより、アンテナ部201から再放射される電波の振幅及び位相を変化させることで、この振幅及び位相の変化により情報を伝達することができる。

【0106】(11) クロック生成部214

クロック生成部214は、基準時刻を示す基準クロックを繰り返し生成し、生成した基準クロックを制御部209へ出力する。

(12) 入出力部215

入出力部215は、制御部209からアクセス命令とアクセス情報を受け取る。アクセス命令は、Read命令及びWrite命令からなる。アクセス命令がRead命令である場合には、アクセス情報は、物理アドレスと読み出しバイト数を含み、アクセス命令がWrite命令である場合には、アクセス情報は、物理アドレスと書き込みバイト数と書込み内容を含む。

【0107】入出力部215は、アクセス命令がRead命令である場合には、メモリ部216の前記物理アドレスにより示される位置から、前記読み出しバイト数分の情報を読み出し、読み出した情報を制御部209へ出力する。入出力部215は、アクセス命令がWrite命令である場合には、メモリ部216の前記物理アドレスにより示される位置から、前記書込みバイト数分、前記書込み内容を書き込み、書込み終了の情報を制御部209へ出力する。

【0108】ここで書込み終了の情報とは、書込みが正常に終了したか否かを示し、正常に終了していない場合には、さらに、その理由を示す情報を含む。

(13) アンテナ部201

アンテナ部201は、受信アンテナであり、電波を受信し、受信した電波を電力信号に変換して、電力信号を復調部206及び電源部203へ出力する。また、受信した電波を反射(再放射)する。

1.6 管理装置400の構成

管理装置40a及び40bは、同様の構成を有する。また、携帯電話型リーダライタ30c、携帯電話内蔵型管理装置40d及び携帯端末型リーダライタ30eは、管理装置40aと同様の構成を内蔵する。ここでは、これらの装置を管理装置40として説明する。

【0109】管理装置40は、図21に示すように、情報記憶部401、制御部402、LAN接続部403及び出入力部404から構成され、具体的には、マイクロプロセッサ、ハードディスク、ROM(Read Only Memory)、RAM(Random Access Memory)などから構成される。

(1) 出入力部404

出入力部404は、リーダライタ30の出入力部101と接続されており、制御部402から出入力命令と出入力情報とからなる組を受け取り、受け取った出入力命令と出入力情報とからなる組を出入力部101へ出力する。

【0110】また、出入力部404は、出入力部101からアクセス応答命令とアクセス応答情報と識別コードとを受け取り、受け取ったアクセス応答命令とアクセス応答情報と識別コードとを制御部402へ出力する。

(2) 制御部402

制御部402は、出入力命令と出入力情報とからなる組を生成し、生成した出入力命令と出入力情報とからなる組を出入力部404へ出力する。

【0111】出入力命令は、入力命令又は出力命令からなる。入力命令は、無線ICタグのメモリからデータを読み出す命令であり、出力命令は、無線ICタグのメモリにデータを書き込む命令である。出入力命令が入力命令である場合に、出入力情報は、無線ICタグのメモリの物理アドレスと読み出バイト数とを含む。出入力命令が出力命令である場合に、出入力情報は、無線ICタグのメモリの物理アドレスと書き込みバイト数と書込み内容とを含む。

【0112】制御部402は、平文を暗号鍵を用いて暗号化して暗号文を生成する暗号アルゴリズムE2と、前記暗号アルゴリズムE2により生成された暗号文を復号鍵を用いて解読して平文を生成する復号アルゴリズムB2とを有している。ここで、この暗号アルゴリズムE2は、前記暗号アルゴリズムE1とは別の暗号アルゴリズムである。なお、同一の暗号アルゴリズムであるとしてもよい。

【0113】制御部402は、入力命令に対応する入力情報を生成する際に、「メカ名」や「運送業者名」などの入力情報を前記暗号鍵を用いて暗号アルゴリズムE2により暗号化して暗号文を生成し、生成した暗号文を入力情報とする。なお、暗号化しないとしてもよい。また、制御部402は、出入力部404からアクセス応答命令とアクセス応答情報と識別コードとを受け取り、受

け取ったアクセス応答命令が、入力命令に対応する場合に、アクセス応答情報を前記復号鍵を用いて復号アルゴリズムB2により復号して平文を生成し、アクセス応答情報としての生成した前記平文と識別コードとを情報記憶部401へ書き込む。なお、暗号化されていないアクセス応答情報については、復号しないとしてもよい。

【0114】また、制御部402は、LAN接続部403を介して、ホストコンピュータ60から情報を受け取り、受け取った情報を情報記憶部401へ書き込む。また、情報記憶部401に記憶されている情報を、LAN接続部403を介して、ホストコンピュータ60へ出力する。

(3) 情報記憶部401

情報記憶部401は、各種の情報を記憶する。

【0115】(4) LAN接続部403
LAN接続部403は、制御部402とLAN装置70とを接続する。

(5) 携帯電話型リーダライタ30c、携帯電話内蔵型管理装置40d及び携帯端末型リーダライタ30eの構成

携帯電話型リーダライタ30c、携帯電話内蔵型管理装置40d及び携帯端末型リーダライタ30eは、管理装置40と同様の構成を内蔵する。ここでは、管理装置40との相違点について簡単に説明する。

【0116】携帯電話型リーダライタ30c及び携帯電話内蔵型管理装置40dは、LAN接続部403を備える代わりに、携帯電話機能を有し、携帯電話機能により、基地局50、公衆回線網、受信装置51、接続装置53及びLAN装置70を介して、ホストコンピュータ60と接続される。また、携帯端末型リーダライタ30eは、LAN接続部403を備える代わりに、ICカード52が装着され、ICカード52により、管理装置40e及びLAN装置70を介して、ホストコンピュータ60と接続される。

1.7 ホストコンピュータ60の構成

ホストコンピュータ60は、図21に示すように、制御部601、LAN接続部602、DB更新部603及びデータベース61から構成されている。具体的には、マイクロプロセッサ、ハードディスク、ROM、RAMなどから構成される。

【0117】(1) データベース61

データベース61は、オープンデータ部とクローズドデータ部とから構成され、オープンデータ部とクローズドデータ部とは、それぞれ生産データ部、物流データ部、販売データ部、サービスデータ部、回収リサイクルデータ部から構成されている。

【0118】データベース61に記憶されている情報の一例を、図22に示す。この図に示すように、オープンデータ部の生産データ部には、「分解方法」、「部品データ」と「有毒情報」が記憶されている。オープンデ

ータ部の回収リサイクルデータ部には、「リサイクル活用情報」が記憶されている。また、クローズドデータ部の生産データ部には、「検査情報」が記憶されている。物流データ部には、「追跡記録」が記憶されている。販売データ部には、「POS情報」及び「販売先情報」が記憶されている。サービスデータ部には、「品質情報」が記憶されている。回収リサイクルデータ部には、「マニフェスト情報」が記憶されている。

【0119】(2) DB更新部603

10 DB更新部603は、制御部601の指示により、データベース61に情報を書き込み、又は、データベース61から情報を読み出す。

(3) 制御部601

制御部601は、DB更新部603を介して、データベース61に情報を書き込み、又は、データベース61から情報を読み出す。

【0120】また、LAN接続部602を介して、管理装置40と接続され、管理装置40から情報を受け取り、データベース61に受け取った情報を書き込む。また、データベース61から読み出した情報を管理装置40へ出力する。

(4) LAN接続部602

LAN接続部602は、制御部601とLAN装置70とを接続する。1.8 リーダライタ30及び無線ICタグ80の動作リードライタ30及び無線ICタグ80の動作について説明する。

【0121】(1) リーダライタ30及び無線ICタグ80の概要動作

リーダライタ30及び無線ICタグ80の概要動作について、図23に示すフローチャートを用いて説明する。同期信号送信期間において、制御部102は、同期信号送信命令を出し、生成した同期信号波を出し、命令生成部104は、同期信号送信命令に基づいて、パルス信号波を生成して出し、同期信号波に基づいて、パルス信号波を生成して出し、変復調部111は、搬送波の振幅を変化させ、振幅の変化した搬送波を出し、アンテナ部112は、搬送波を電波として空間に放射する。制御部208は、アンテナ部201、復調部206、6、命令解読部207を介して、同期信号送信命令を受け取り、さらに同期信号波を受信し、同期信号を抽出し、抽出した同期信号に同期する同期信号を繋り返し含む同期信号波を生成する(ステップS102)。

【0122】制御部102は、識別コード収集命令を出し、命令生成部104は、パルス信号波を生成して出し、変復調部111は、搬送波の振幅を変化させ、振幅の変化した搬送波を出し、アンテナ部112は、搬送波を電波として空間に放射する。制御部209は、アンテナ部201、復調部206、命令解読部207を介して、識別コード収集命令を受け取る(ステップS103)。

【0123】制御部102は、3秒間の識別コード収集期間の経過を監視し（ステップS104）、3秒間の識別コード収集期間において、各無線ICタグから識別コードを収集する（ステップS105）。識別コード収集期間が経過すると（ステップS104）、制御部102は、各無線ICタグから識別コードの収集が終了したとみなし、識別コードの収集を終了する。

【0124】次に、アクセス期間において、制御部102は、識別コード記憶部106に記憶されている全ての識別コードの読み出しが終了すると（ステップS106）、各識別コードについて、各識別コードにより識別される無線ICタグの領域アクセス認証と領域アクセスとを繰り返し行い（ステップS107）、識別コード記憶部106に記憶されている全ての識別コードの読み出しが終了すると（ステップS106）、処理を終了する。

【0125】(2) 無線ICタグの識別コードの収集の動作

ここでは、図23のフローチャートのステップS105に示す無線ICタグの識別コードの収集の動作について、図24に示すフローチャートを用いて説明する。制御部209は、乱数生成部211に対して乱数を生成するように指示し、乱数生成部211は、乱数R0を生成し（ステップS131）、ハッシュ部212はハッシュ値を生成し、制御部209は、識別コード記憶部208から識別コードを読み出し、ハッシュ部212からハッシュ値を受け取り、受け取ったハッシュ値をチャネル番号とするチャネルを選択し（ステップS132）、識別コード送信期間において、選択したチャネルにより（ステップS133）、読み出した識別コードと乱数R0と識別コード送信命令とを変調部213及びアンテナ部201を介してリードライタ30へ送信し、アンテナ部112、変調部111及び命令解読部110を介して、制御部102は、識別コード送信命令と識別コードとを受け取り、ハッシュ部109は、乱数R0を受け取り（ステップS134）、ハッシュ部109は、ハッシュ値を生成し、制御部102は、受け取った識別コードを一時記憶部103に書き込み、生成されたハッシュ値をチャネル番号とするチャネルを選択し（ステップS135）、制御部102は、識別コード応答期間内の選択したチャネルにおいて（ステップS136）、前記識別コードと識別コード応答命令とを命令生成部104、変調部111及びアンテナ部112を介して送信し（ステップS138）、制御部209は、アンテナ部201、変調部206及び命令解読部207を介して、識別コード応答期間において、選択したチャネルにより（ステップS137）、識別コード応答命令と識別コードとを受け取り（ステップS138）、制御部209は、識別コード記憶部208から読み出した識別コードと、受け取った識別コードとを比較し、一致しているなら（ステッ

プS139）、識別コード一致期間において、選択したチャネルにより（ステップS140）、識別コードと識別コード一致命令とを、変調部213及びアンテナ部201を介して出力する（ステップS142）。一致していないなら（ステップS140）、ステップS131へ戻って、処理を繰り返す。

【0126】制御部102は、識別コード一致期間内の選択したチャネルにおいて（ステップS141）、アンテナ部112、変調部111、命令解読部110を介して、識別コード一致命令を受け取り（ステップS142）、一時記憶部103から前記識別コード読み出し、読み出した識別コードを識別コード記憶部106へ書き込む（ステップS143）。

【0127】(3) 無線ICタグの領域アクセス認証及び領域アクセスの動作

ここでは、図23のフローチャートのステップS107に示す無線ICタグの領域アクセス認証と領域アクセスの動作について、図25に示すフローチャートを用いて説明する。制御部102は、アクセス期間において、識別コード記憶部106から1個の識別コードを読み出し（ステップS161）、アクセス要求命令と前記読み出した識別コードとを、命令生成部104、変調部111及びアンテナ部112を介して出力し、制御部209は、アクセス期間において、アンテナ部201、復調部206及び命令解読部207を介して、識別コードとアクセス要求命令とを受け取り（ステップS162）、制御部209は、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較し、一致しなければ（ステップS163）、さらにアクセス要求命令の受け取りを待ち受ける。一致すれば（ステップS163）、制御部209は、乱数生成部211に対して乱数を生成するように指示し、乱数生成部211は、乱数R0を生成し（ステップS164）、暗号化部108は、鍵記憶部231から領域鍵K1～K6を読み出し、読み出した領域鍵K1～K6を用いて、乱数R0に暗号アルゴリズムE1を施して、それぞれ暗号化乱数R1～R6を生成し、生成した暗号化乱数R1～R6を生成乱数記憶部234に書き込む（ステップS166）。

【0128】制御部209は、識別コードと乱数R0と認証子応答命令とを変調部213及びアンテナ部201を介して出力し、アンテナ部112、変調部111及び命令解読部110を介して、制御部102は、認証子送信命令と識別コードとを受け取り、ハッシュ部109は、乱数R0を受け取り（ステップS165）、ハッシュ部109は、ハッシュ値を生成し、制御部102は、鍵記憶部107に記憶されている領域鍵を読み出し、暗号化部108は、乱数R0を領域鍵を用いて暗号化して暗号化乱数R0'を生成し（ステップS167）、制御部102は、命令生成部104へ前記識別コードと認証子応答命令とを出力し、命令生成部104は、暗号化乱

数R'0」と識別コードと認証子応答命令とを、変復調部111及びアンテナ部112を介して出し、アンテナ部201及び復調部206を介して、命令解読部207は暗号化乱数R'0を受け取り、制御部209は、認証子応答命令と識別コードを受け取り、(ステップS168)、制御部209は、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較し、一致しなければ(ステップS169)、さらに、認証子応答命令の受け取りを待ち受ける。一致すれば(ステップS169)、比較器235は、命令解読部207から受け取った暗号化乱数R'0に一致する暗号化乱数を生成乱数記憶部234から探し、一致する暗号化乱数があれば(ステップS170)、一致する暗号化乱数を識別する番号Xを制御部209へ出力する(ステップS172)。一致する暗号化乱数がなければ(ステップS170)、比較器235は、暗号化乱数が一致しない旨を制御部209へ出力し、制御部209は、識別コードとアクセス不許可命令と理由コードとを、変調部213及びアンテナ部201を介して出力する(ステップS171)。

【0129】制御部102は、前記識別コードとアクセス情報とアクセス命令とを、命令生成部104、変復調部111及びアンテナ部112を介して出し、制御部209は、アクセス命令と識別コードとアクセス情報とを、アンテナ部201、復調部206及び命令解読部207を介して受け取る(ステップS173)。制御部209は、次に、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較し、一致しなければ(ステップS174)、さらに、アクセス命令の受け取りを待ち受ける。一致すれば(ステップS174)、制御部209は、アクセス情報に含まれる物理アドレスが番号Xで示されるステージ領域内を示しているか否かを判断し、ステージ領域内を示していない場合には(ステップS175)、識別コードとアクセス不許可命令と理由コードとを、変調部213及びアンテナ部201を介して出し、制御部102は、アンテナ部112、変復調部111及び命令解読部110を介して、識別コードとアクセス不許可命令と理由コードとを受け取る。

【0130】ステージ領域内を示している場合には(ステップS175)、制御部209は、アクセス命令とアクセス情報を入出力部215へ出力し、入出力部215は、制御部209からアクセス命令とアクセス情報を受け取り、アクセス命令とアクセス情報をに基づいてメモリ部216にアクセスを行い、制御部209は、そのアクセスの結果に基づいて、アクセス応答情報を生成し(ステップS177)、識別コードとアクセス応答命令とアクセス応答情報をと、変調部213及びアンテナ部201を介してへ出力し、制御部102は、アンテナ部112、変復調部111及び命令解読部110を介し

て、アクセス応答命令とアクセス応答情報を識別コードとを受け取り(ステップS178)、入出力部101は、アクセス応答命令とアクセス応答情報を識別コードとを受け取り、管理装置40へ受け取ったアクセス応答命令とアクセス応答情報を識別コードとを出力する。

1.9 無線ICタグの種類と適用分野無線ICタグ80は、搬送周波数として、2.4～2.5GHzの準マイクロ波帯を使用し、電波方式により通信を行っている。

【0131】また、無線ICタグ80は、8.60MHz～9.15MHzのUHF帯を使用し、同様に電波方式により通信を行うようにしてもよい。この場合、タグ寸法は、一例として、長さ100mm、幅15mm、厚さ0.5mmである。このとき、通信可能な距離は、2～3mであり、通信速度は、10～20m秒/biteである。

【0132】この他に、磁気方式(電磁誘導方式)による無線ICタグが知られており、使用される周波数は、1.25KHz又は1.3.5.6MHzであり、寸法は、縦6cm、横8cmであり、通信距離は、50cm以内であり、通信速度は、数Kbpsである。また、重ね読みはできない、又は3枚程度以内まで可能である。電波方式は、磁気方式よりも高周波を用いるので、アンテナを小さくでき、タグを小型化できる。

【0133】無線ICタグの適用分野と、タグ単価と、通信距離との関係を図26に示す。この図では、横軸にタグ単価ととり、縦軸に通信距離をとっている。タグ単価が数円から500円程度であり、通信距離が数10cm以上である範囲A10は、前記の電波方式を用いる無線ICタグの適用範囲を示し、この範囲内における用途として、宅配A2.5、郵便A2.2、航空荷物A2.3、洗濯機管理A2.4、ライフサイクルマネージメントA2.1及び車両管理A2.6がある。

【0134】また、タグ単価が10円～500円であり、通信距離が50cm以内である範囲A11は、前記磁気方式(1.3MHz帯)を用いる無線ICタグの適用範囲を示し、この範囲内における用途として、OA機器用消耗品管理A3.1、イモビライザA3.0、テレホンカードA3.2及び定期券A2.9がある。また、タグ単価が10円以下であり、通信距離が数10cm程度である範囲A2.7において、共振タグが知られており、万引き防止のために用いられている。1.10 その他の変形例なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は上記実施の形態に限定されないのはもちろんである。すなわち、以下のようの場合も本発明に含まれる。

【0135】(1) 図3に示す衣服90に付されている無線ICタグ80bは、図18に示すように、非プロテクト部のサービスステージ領域に、「洗濯方法」が記録されている。家庭用電気洗濯機500は、図27に示すように、洗濯槽内上部501において、リーダライタ3

0と同様のリーダライタを内蔵しており、また、様々な洗濯方法に応じた洗濯コースを記憶している。衣服90が洗濯槽内に入れられると、家庭用電気洗濯機500が内蔵するリーダライタは、無線ICタグ80bの非プロトコル部のサービスステージ領域に記録されている「洗濯方法」を読み出し、家庭用電気洗濯機500は、読み出した洗濯方法に応じた洗濯コースを読み出し、読み出した洗濯コースにより、洗濯を開始する。

【0136】また、食材に無線ICタグが添付され、この無線ICタグは、調理方法を非プロトコル部のサービスステージ領域に記録しており、電子レンジなどの調理器は、リーダライタ30と同様のリーダライタを内蔵しており、また、様々な調理方法に応じた調理コースを記憶している。無線ICタグの添付された食材が内部に入れられるごとに、調理器が内蔵するリーダライタは、無線ICタグの非プロトコル部のサービスステージ領域に記録されている「調理方法」を読み出し、調理器は、読み出した調理方法に応じた調理コースを読み出し、読み出した調理コースにより、食材を調理する。

【0137】(2)メモリ部216は、5個のステージ領域を有するとしているが、5個に限定されることはない。5個より多いステージ領域を有するとしてもよいし、5個より少ないステージ領域を有するとしてもよい。また、無線ICタグ80のメモリ部216内の可変部は、この領域内に情報が埋め尽くされれば、可変部の先頭から再度上書きするとしてもよい。

【0138】また、図28に示すように、非プロトコル部とプロトコル部とから構成され、プロトコル部は、生産ステージ領域と物流ステージ領域と販売ステージ領域とサービスステージ領域と回収リサイクルステージ領域と拡張領域とから構成されるとしてもよい。拡張領域は、各ステージ領域内に情報が埋め尽くされた場合に、さらに情報を書き込む領域として用いられる。

【0139】(3)リーダライタが、同一時間帯内において、1個の無線ICタグのみに対して読み書きを行う場合には、図23に示す処理を行なう代わりに、図29に示すフローチャートに示すようにして、ステージ領域の認証とステージ領域へのアクセスを行うようとしてもよい。リーダライタは、アクセス要求を無線ICタグG送信する(ステップS202)。無線ICタグは、乱数R0を生成し(ステップS203)、生成した乱数R0をリーダライタへ出力する(ステップS204)。リーダライタは、暗号化乱数R'0=E1(R0,K1)を生成し(ステップS206)、生成した暗号化乱数R'0を無線ICタグに送信する(ステップS207)。無線ICタグは、暗号化乱数R'0=E1(R0,K1)、R2=E1(R0,K2)、…、R6=E1(R0,K6)を生成し(ステップS208)、受け取った暗号化乱数R'0が、R1～R6のいずれかに一致するか否かを判断し、一致しない場合に(ステップS208)、

「アクセス不許可」をリーダライタへ送信し(ステップS209)、一致する場合に(ステップS208)、ステージ領域を識別するX_iを決定する(ステップS210)。リーダライタは、領域X_3へのアクセスを行なうアクセス命令を無線ICタグへ送信する(ステップS211)。無線ICタグは、X_iとX_3とが一致するか否かを判断し、一致しない場合に(ステップS212)、リーダライタに「アクセス不許可」を送信する(ステップS213)。一致する場合に(ステップS212)、前記アクセス命令に基づいて無線ICタグが有するメモリにアクセスし(ステップS214)、アクセス結果をアクセス応答としてリーダライタへ送信する(ステップS215)。

【0140】(4)無線ICタグ80は、上記に説明したように、搬送周波数として、2.4～2.5GHzの準マイクロ波帯を使用し、電波方式により通信を行うとしているが、搬送周波数として、2.4～2.5GHzの準マイクロ波帯及び860MHz～915MHzのUHF帯両方を使用し、同様に電波方式により通信を行うとしてもよい。

【0141】また、無線ICタグ80を使用するステージに応じて、リーダライタ30は、使用的する搬送周波数としてUHF帯又は準マイクロ波帯のいずれかを選択するようとしてもよい。例えば、リーダライタ30と無線ICタグ80との距離が一定して近接している生産工場内においては、通信距離の短い準マイクロ波帯を選択し、リーダライタ30と無線ICタグ80との距離が一定しないと考えられる物流ステージ内においては、通信距離の長いUHF帯を選択するようとしてもよい。

【0142】(5)上記の実施の形態においては、同一期間において複数の無線ICタグへのアクセスを行なうマルチ読み取りを行う際に、識別コード収集期間において、時分割方式により識別コードを収集し、アクセス期間においては、リーダライタ30は、各無線ICタグについて順番にアクセスするとしているが、アクセス期間においても時分割方式により、リーダライタ30は、各無線ICタグにアクセスするとしてもよい。

【0143】また、識別コード収集期間は、第1収集期間と第2収集期間との2個の収集期間を含み、第1収集期間と第2収集期間において、識別コードを収集するとしているが、識別コード収集期間は、3個以上の収集期間を含み、それぞれの収集期間において、識別コードを収集するとしてもよい。また、搬送周波数として、2.4～2.5GHzの準マイクロ波帯を周波数分割して、分割された各局波数を複数の無線ICタグに割り当てる、リーダライタ30は、分割された各局波数を用いて、各無線ICタグにアクセスするとしてもよい。

【0144】また、スペクトラム拡散技術に基づくCDMA(Code Division Multiple Access)方式を用いるとしてもよい。無線ICタグ毎にそれぞれ異なる拡散コ

ードを設定し、複数の無線ICタグが同一の広帯域無線チャネルを共有する。また、リーダライタ30と各無線ICタグとの間で通信する情報をパケットデータに分割し、各パケットデータの先頭に各無線ICタグを識別する識別コードを付加し、リーダライタ30は、パケットデータを用いて、各無線ICタグにアクセスするとしてもよい。

【0145】(6) 識別コードは、32ビットからなり、製造業者識別コード(10ビット長)と、種類コード(10ビット長)と、製造番号(12ビット長)とから構成されるとしているので、2の32乗個分の識別コードを生成できる。さらに、多くの数の識別コードが必要であれば、識別コードのビット長を増やすとしてもよい。

【0146】また、識別コードを32ビット長とし、さらに、多くの数の識別コードが必要であれば、32ビット長の乱数を生成し、生成した乱数と32ビットの前記識別コードとを加算して、32ビット長の加算結果を得、得られた加算結果を識別コードとしてもよい。この識別コードを用いて無線ICタグとリーダライタとの間で通信を行なうとしてもよい。リーダライタ30により無線ICタグ80にアクセスする場合に、識別コードは、最大50個の無線ICタグを識別できればよいからである。ここで、もちろん加算以外の他の演算を用いるとしてもよい。

【0147】(7) 無線ICタグ80及びリーダライタ30は、記憶している領域鍵が漏洩しないように、無線ICタグ80及びリーダライタ30が記憶している領域鍵を不正に読みだそうとして、無線ICタグ80及びリーダライタ30を分解すると、前記領域鍵を記憶しているメモリが破壊されるタンパク方式を採用するとしてもよい。

【0148】(8) さらに、領域鍵配信装置を設け、領域鍵配信装置は、無線ICタグ80と接続され、6個の領域鍵(K1～K6)を無線ICタグ80内部に書き込むとしている。また、領域鍵配信装置は、リーダライタ30と接続され、2個の領域鍵(K1及びK6、K2及びK6、K3及びK6、K4及びK6又はK5及びK6の何れか)をリーダライタ30内に書き込むとしている。

【0149】この領域鍵配信装置は、リーダライタ30及び無線ICタグ80の製造業者以外の第三者機関が所有し、この第三者機関によりこの領域鍵配信装置を用いて、リーダライタ30及び無線ICタグ80にそれぞれ領域鍵が書き込まれるとしてもよい。これにより、領域鍵のリーダライタ30及び無線ICタグ80への書き込み時点で、領域鍵の漏洩を防ぐことができる。

【0150】(9) すべての領域にアクセスを許すマスタ鍵K7を設け、特別に許された使用者のみにより使用されるリーダライタ30内部にマスタ鍵K7を有し、マ

スタ鍵K7により無線ICタグ80の全ての領域へのアクセスが可能であるとしてもよい。また、前記第三者機関がこの使用者であるとしてもよい。

(10) 上記の実施の形態では、無線ICタグがリーダライタを認証するとしているが、図25に示すフローチャートのステップ161～S170において、リーダライタの処理と無線ICタグの処理とを逆にすることにより、リーダライタが無線ICタグを認証するとしてもよい。これにより、不正に製造された無線ICタグをリーダライタは拒否することができる。

【0151】また、無線ICタグがリーダライタを認証し、かつリーダライタが無線ICタグを認証するとしてもよい。

(11) 販売ステージ領域には、WPCコード(JAN、EAN、UPCコード)を記録するようとしてもよい。ここで、EAN(European Article Numbering System)は、ヨーロッパで使用されている小売食品外装用の国際的な標準コード体系である。UPC(Universal Product Code)は、米国での小売り食品包装用標準バーコードシステムである。また、JANは、1978年にJIS化された共通商品コードで日本で使用されているコード体系である。

【0152】(12) リーダライタは、さらにバーコードを読みのように構成してもよい。また、無線ICタグの樹脂表面にバーコードを印刷して、バーコードの印刷された無線ICタグを製品表面に貼り付けるようにしてもよい。このバーコードの印刷された無線ICタグについて、前記リーダライタは前記バーコードを読み、また、無線ICタグにアクセスするようにしてもよい。

30 【0153】(13) 無線ICタグの貼り付け位置は、ロゴ裏面に限定されない。例えば、テレビジョン受像機の内部に設けられた配線基板の上面に無線ICタグを貼り付けるとしてもよい。このように、無線ICタグの貼り付け位置は、リーダライタ30から送信される電波の届く製品の内部であってもよい。

(14) 店舗で陳列されている商品に無線ICタグを添付し、商店のレジにてリーダライタ30と同様の構成を有する第1のリーダライタを設置し、第1のリーダライタは、正面に對価が支払われた商品に添付されている無線

40 ICタグにその旨を記録し、商店の出入り口にリーダライタ30と同様の構成を有する第2のリーダライタを設置し、第2のリーダライタは、無線ICタグに前記の旨が記録されていない無線ICタグを検出する。これにより、商品の万引きを防止することができる。

【0154】(15) 衣服の製造業者は、その製造業者名を記録している無線ICタグを製造した衣服に添付し、仕入れ業者は、無線ICタグに記録されている製造業者の名をリーダライタ30により読み出すことにより、衣服の製造業者名を確認することができる。これにより、ニセモノを誤って購入することを防止できる。ま

た、高級衣料品や高級装飾品などの高級ブランド品に、無線ICタグを添付することにより、高級ブランド品の偽物の流通を防止することができる。また、高級ブランド品の品質を保証することができる。また、流通経路において、経路情報を無線ICタグに書き込むことにより、流通の経路の管理、探索ができる。

【0155】(16) 生産現場において、生産従事者は、その者の名前が記録されている無線ICタグが裏面に添付されている名札を身につけ、生産現場の各所において、リーダライタ30と同様の構成を有するリーダライタが設置され、このリーダライタは、無線ICタグに記録されている名前を読み出し、その場所とともに記録する。これにより、生産現場における人の動きの管理をすることができる。また、小売店などにおいても同様である。

【0156】(17) 病院において、患者が入院し、治療を受け、退院に至るまでにおいて、上記の製品のライフルサイクルと同様に、病院の療養サイクルにおける複数のステージ、すなわち、入院、検査、手術、治療、養生、投薬、会計、退院などを経る。これらの複数のステージ毎に、それぞれ必要な情報が存在する。患者は、無線ICタグを身につける。無線ICタグは、ステージ毎のステージ領域に有している。入院ステージ領域には、患者の名前及び病状情報が書き込まれ、検査ステージ領域には、検査結果が書き込まれ、手術ステージ領域には、手術方法及び結果が書き込まれ、治療ステージ領域には、治療方法及び結果などの処置情報が書き込まれ、養生ステージ領域には、養生中の病状情報が書き込まれ、投薬ステージ領域には、患者に投薬された医薬品に関する情報が書き込まれ、会計ステージ領域には、治療、投薬などの保険点数及び金額情報が書き込まれ、退院ステージ領域には、退院時点における病状情報が書き込まれている。各ステージ領域にアクセスできる権限を有する者は限定されている。病院内の病室、治療室、手術室、会計室などの各所において、リーダライタ30と同様の構成を有する各ステージのリーダライタが設置され、各ステージのリーダライタを操作する権限を有する者、例えば、患者、医者、看護師又は会計担当者などは、自分だけが秘密に知っているパスワードをリーダライタに入力し、正しく権限を有する者である場合には、リーダライタは、無線ICタグの各ステージ領域から情報を読み出し、又は情報を書き込む。

【0157】これにより、患者は、自分の病状や治療方法について正しい知識を得ることができる。また、医者又は看護師が患者を取りえたり、処置を誤ったりすることを防止ができる。また、会計担当者は、正確に治療代金などを計算できる。

(18) 物流ステージにおいて、図7に示すように、物流管理サブシステム20bに含まれる第3組のリーダライタ30d及び携帯電話内蔵型管理装置40dが、貨物

トラックに搭載され、アンテナ部を有するリーダライタ30dが、貨物トラックの荷物搬入口の上部内側に設置されているので、荷物搬入口近辺の無線ICタグの添付された貨物の内容物を無線ICタグに記録されている情報を読み出すことにより知ることができます。こうして得られた貨物の内容物についての情報と現在トラックが位置している場所の情報をと、基地局50、公衆回線、受信装置51、接続装置53、LAN装置70を介して、ホストコンピュータ60のデータベース61に書き込む。

【0158】これにより、貨物トラックに搬入された貨物又は貨物トラックから搬出された貨物の内容物とその位置とを時々刻々と知ることができるので、貨物の流通ルートを確実に把握することができる。

(19) 無線ICタグが本、CD、衣服などに添付され、これらの本、CD、衣服などが重なり合って保管されている場合においても、リーダライタ30は、これら複数の無線ICタグとのアクセスを行なうことができるので、これらの本、CD、衣服などの在庫管理ができる。

【0159】(20) オフィスに複数台設置されているコンピュータやプリンタなどを接続する複数の配線毎に、前記配線を接続する機器と機器とを示す情報が記録されている無線ICタグを添付し、これらの複数の配線をオフィスの床下に埋め込む。リーダライタを床上から操作して、これらの無線ICタグに記録されている情報を読み出すことにより、機器と機器とを接続する配線の位置を知ることができる。

【0160】(21) 自動車の車体に無線ICタグを添付し、サービスステージ領域に、自動車の運行状況、例えば、走行距離と日付、給油量と日付などを定期的に無線ICタグに記録するようにしてよい。また、自動車の修理履歴を記録して管理するようにしてよい。また、自動車が故障とされたときに、これらの情報を用いて、自動車の部品、モジュールのリユースを決定するようにしてよい。

【0161】】このようにして、廃棄される物品のリユースが簡単に決定できるので、廃棄される物品の回収率が向上し、さらに、物品が再利用されるリユース率が向上する。

(22) 無線ICタグに、さらに、温度センサ、圧力センサなどのセンサを付加し、これらのセンサにより、定期的に、無線ICタグの周辺の温度、圧力を検出し、検出した温度、圧力を無線ICタグ内に記録するようにしてよい。また、この無線ICタグは、これらのセンサを駆動させるため電池を備えているとしてもよい。

【0162】(23) 家庭内に用いられる電化製品や衣服に無線ICタグが添付され、リーダライタを用いて、家庭内に存在するこれらの電化製品や衣服に添付されている無線ICタグに記録されている情報を読み出すこと

により、家庭内資産管理を行うことができる。

(24) 上記実施の形態では、秘密鍵方式による暗号を用いているが、公開鍵方式による暗号を用いるとしてもよい。例えば、楕円曲線上の離散対数問題を安全性の根拠とする暗号通信方式を用いてもよい。

2 第2の実施の形態

図30は、本発明における第2の実施の形態のライフサイクル管理システムのライフサイクル工程を示した図である。以下、図30に示すように、製品のライフサイクルの工程を生産工程Q23、物流工程Q24、販売工程Q25、使用工程Q26、回収処理工程Q27の5つの工程に分けて説明するが、ライフサイクルの工程はこれに限るものではない。例えば、図30に示すように、使用工程と回収処理工程の間に再生工程Q28を設けてよい。

【0163】図30に示すように、各工程内あるいは各工程同士において製品Q1の管理システムは、製品Q1に関する製品情報を製品Q1の外部に取り付けられた非接触式通信を行うICタグQ2にメモリを設け、各工程ごとに設けられた無線通信を行うリーダライタQ3を用いて、メモリに製品情報を各工程ごとに書き込んだり、または、書き込まれた製品情報を読み出したりすることにより行うものである。

【0164】なお、製品Q1としては、電気業界における家庭電化製品、コンピュータ等の電子機器あるいは電子部品、産業用機器、また車両業界における自動車、モーターサイクル等、あるいはこれらの部品、食品業界における梱包された食品等、また住宅業界における住宅建材、家具等、また衣料業界における衣服等、その他、靴、靴、食器あるいは雑貨等の様々な業界の製品がある。

【0165】なお、以下の実施の形態では、情報記憶媒体の一例として、ICタグを用いる。また、ICタグQ2は、製品Q1あるいは製品Q1に用いられている個々の部品を取り付けられる。特に、製品Q1に付された社章、商標あるいはマークなどのロゴタイプと製品Q1の間、または、そのロゴタイプの周辺部分に設けることにより、ICタグQ2は外部から目立つことが無くなり、製品Q1の外観を損なうことなくとともに、ICタグQ2の所在を統一することができ、各工程において、ICタグQ2の所在を明確にすることができます。

【0166】次に、図31において、本発明における第2の実施の形態に係るライフサイクル管理システムの通信システムについて説明する。図31は、本発明における第2の実施の形態に係る非接触のICタグQ2aの構造およびリーダライタQ3を示すブロック図を表している。以下、非接触のICタグは、そのICタグに製品情報の書き込みあるいは製品情報の読み出しを行なうリーダライタと電波により通信が行なわれる。

【0167】図31に示すように、ICタグQ2aは、

アンテナQ4、電源回路Q5、復調回路Q6、制御回路Q7、メモリQ8aおよび変調回路Q9などで構成されている。まず、リーダライタQ3から暗号化された製品情報の信号が送信され、ICタグQ2aのアンテナQ4で受信し、受信信号は電源回路Q5により電力に変換してICタグQ2aの全装置に電力を供給するとともに、復調回路Q6によって受信信号を復調化する。そして、復調化された信号は、制御回路Q7でその受信信号の内容に応じてメモリQ8aへ書き込みが行われる。

【0168】次に、ICタグQ2aから必要な製品情報を読み出すときは、リーダライタQ3から送信された読み出し信号に対し、ICタグQ2aのアンテナQ4でその読み出し信号を受信する。受信した読み出し信号は、電源回路Q5により電力に変換されるとともに、復調回路Q6により復調化される。そして、復調化された信号に応じて制御回路Q7によってメモリQ8aから必要な製品情報を読み出し、読み出された信号は変調回路Q9により変調されてアンテナQ4から電波信号として送出して読み出しが行われ、リーダライタQ3で製品情報を読み込み、情報に基づき判断を行う。

【0169】ここで、図30に示す5つの各工程におけるICタグQ2aのメモリQ8aに書き込まれる製品情報は、各工程における製品の履歴情報で、以下に示す情報があるがこれに限るものではない。第1の工程である生産工程Q23においてICタグQ2aに書き込まれる製品情報としては、製造元に関するメーカー名、品名、品番、製品番号、製品が作られた年月日または時刻、製品が製造された工場、製品に関する材料、製法および製造の条件、製品の部品の保証期間等がある。

【0170】第2の工程である物流工程Q24においてICタグQ2aに書き込まれる製品情報としては、製品の出入庫日、グローバルロケーション番号および運送業者名等がある。第3の工程である販売工程Q25においてICタグQ2aに書き込まれる製品情報としては、ユーザーに販売したときの製品保証に関する情報(すなわち保証開始日、販売元保証等)、保証書番号、館に関する卸業者名と館日、ユーザーに販売した小売店名と販売日がある。

【0171】第4の工程である使用工程Q26においてICタグQ2aに書き込まれる製品情報としては、使用された製品が故障したときの故障箇所、故障内容、修理した回数、修理日、修理部品、修理内容等の修理記録や製品を修理した修理会社や修理者名等がある。第5の工程である回収処理工程Q27においてICタグQ2aに書き込まれる製品情報としては、その製品を回収した回収日、再利用するための部品名、処理方法、処理年月日、処理業者、処理者等のリユースに関する記録、製品を回収した回収業者名または製品を廃棄した廃棄業者名等がある。

【0172】また、第2の実施の形態においてライフサ

イクルの各工程においてメモリQ 8 aに書き込まれる製品情報に、書き込むことに書き込まれたときの年月日および時刻情報を含ませておくことで、リーダライタQ 3により新たな製品情報をメモリQ 8 aに書き込む際、メモリQ 8 aのメモリの容量が不足して、その新たな製品情報がメモリQ 8 aに書き込むことができないときは、最も古い製品情報を自動で削除して、新たな製品情報をメモリQ 8 aに書き込むことができるようすることもできる。

【0173】なお、この場合、リーダライタQ 3の使用者に書き込まれた製品情報のリストをリーダライタQ 3に送信することにより、使用者にどの製品情報を削除するかを選択させて、一番不要な製品情報を削除することも可能である。

3 第3の実施の形態

次に、本発明における第3の実施の形態に係るライフサイクル管理システムについて説明する。第3の実施の形態において、ライフサイクル工程は第2の実施の形態と同じなので図3 0を用いて説明し、第3の実施の形態におけるICタグの構造を図3 2に示し、図3 1と同じ構成のものには同じ符号を付し、説明を省略する。

【0174】第3の実施の形態において、図3 0に示す5つの各工程における製品情報は、各工程において共通の情報として共有化された共通製品情報と、各工程間ににおいて共有化しないで各工程内で閉ざされた非共通製品情報とに分けられており、これにより製品情報の各工程同士でのセキュリティを囲り、特定の者のみが非共通製品情報を得ることができるものである。

【0175】図3 0における各工程での共通製品情報および非共通製品情報の分け方の1つとして、以下に示す。第1の工程である生産工程Q 2 3においてICタグQ 2 bに書き込まれる共通製品情報としては、製造元に関するメーカー名、品名、品番、製品番号等および製品が作られた年月日または時刻、製品や部品の保証期間等があり、また、非共通製品情報としては、製品が製造された工場、製品に関する材料、製法および製造の条件等がある。

【0176】第2の工程である物流工程Q 2 4においてICタグQ 2 bに書き込まれる共通製品情報としては、製品の入出庫日やグローバルロケーション番号等があり、また、非共通製品情報としては、運送業者名等がある。第3の工程である販売工程Q 2 5においてICタグQ 2 bに書き込まれる共通製品情報としては、ユーザーに販売したときの製品保証に関する情報（すなわち保証開始日や販売元保証）、保証書番号等があり、非共通製品情報としては、御にに関する御業者名や御日、ユーザーに販売した小売店名や販売日がある。

【0177】第4の工程である使用工程Q 2 6においてICタグQ 2 bに書き込まれる共通製品情報としては、使用された製品が故障したときの故障箇所、故障内容

10 【0178】なお、上述した各工程の共通製品情報および非共通製品情報は、製品に応じて、または、ライフサイクル管理システムの管理形態において決めればよく、上述の共通製品情報を非共通製品情報として扱ったり、非共通製品情報を共通製品情報と扱うこともあり、これらに限ったものではない。次に、図3 2を用いて、各工程の共通製品情報および非共通製品情報のセキュリティが施された第3の実施の形態におけるICタグQ 2 bとリーダライタQ 3の通信システムについて説明する。

【0179】第3の実施の形態と第2の実施の形態が異なる点は、図3 2に示すように、ICタグQ 2 bのメモリ8 bの領域が、共通製品情報を記憶する共通製品情報メモリ部Q 1 0および非共通製品情報を記憶する非共通製品情報メモリ部Q 1 1に分けられていることである。まず、ICタグQ 2 bに製品情報を書き込むときは、リーダライタQ 3の使用者は、製品情報を共通製品情報あるいは非共通製品情報にするかを選択して暗号化された製品情報の信号および共通製品情報メモリ部Q 1 0あるいは非共通製品情報メモリ部Q 1 1のどちらに書き込むかを指定するメモリ指定情報の信号をICタグQ 2 bに30送信する。

【0180】ICタグQ 2 bはその暗号化された製品情報の信号をアンテナQ 4で受信し、受信信号は電源回路Q 5により電力に変換してICタグQ 2 bの全装置に電力を供給するとともに、復調回路Q 6により受信信号を復調化する。このとき復調化された信号には、共通製品情報メモリ部Q 1 0あるいは非共通製品情報メモリ部Q 1 1のどちらに書き込むかを指定するメモリ指定情報が含まれているので、そのメモリ指定情報に従って、指定された共通製品情報メモリ部Q 1 0あるいは非共通製品情報メモリ部Q 1 1に、制御回路Q 7により、受信信号の内容の書き込みが行われる。

【0181】次に、ICタグQ 2 bから共通製品情報を読み出すときは、リーダライタQ 3の使用者は、無条件でICタグQ 2 bと通信でき、リーダライタQ 3から共通製品情報を読み出す信号を含む信号をICタグQ 2 bに送信する。アンテナQ 4から受信した共通製品情報を読み出す信号は、電源回路Q 5により電力となるとともに、復調回路Q 6により復調化され、制御回路Q 7によってメモリ8 bの共通製品情報メモリ部Q 1 0から必要50な共通製品情報を読み出し、変調回路Q 9を通してアン

テナQ4から電波信号として送出して、リーダライタQ3で共通製品情報を受信する。

【0182】また、ICタグQ2bから非共通製品情報を読み出すときは、まず、リーダライタQ3の使用者は、非共通製品情報メモリ部Q11とアクセスするためには非共通製品情報メモリ部Q11を指定する信号、すなわち暗号鍵をICタグQ2bに送信する。そして、暗号鍵により非共通製品情報を読み出しが可能となったとき、リーダライタQ3から必要な非共通製品情報を読み出す信号をICタグQ2bに送信する。

【0183】アンテナQ4から受信した非共通製品情報を読み出す信号は、電源回路Q5により電力となるとともに、復調回路Q6により復調化され、制御回路Q7によってメモリ部8bの非共通製品情報メモリ部Q11から必要な非共通製品情報を読み出される。読み出された非共通製品情報の信号は復調回路Q9を通してアンテナQ4から電波信号として送信され、リーダライタQ3で非共通製品情報を受信する。

【0184】このように、第3の実施の形態は、少なくとも非共通製品情報メモリ部Q11に書き込まれた非共通製品情報を読み出すときは、リーダライタQ3からICタグQ2bに送信する読み出し信号に非共通製品情報メモリ部Q11を指定する信号、すなわち暗号鍵が信号に含まれていないと制御回路Q7が判断した場合は、その読み出し信号は、メモリ部8bにアクセスできないようプロテクトされているものである。

【0185】各工程におけるリーダライタはそれぞれ別の暗号鍵をもっているため、この暗号鍵の存在により、特定の使用者のみが非共通製品情報を得ることができるシステムとなっている。なお、この暗号鍵は、メモリにアクセスするための手段を意味し、暗号コード信号であったり、パスワードによる信号等である。また、カオス理論を用いたブロック信号やスリーム信号等もある。これは以下の実施の形態についても同様である。

【0186】すなわち、暗号鍵が存在するときにのみリーダライタとメモリが通信可能となるので、製品情報のセキュリティを図ることができる。また、第3の実施の形態において、暗号鍵が、パスワード入力による信号とした場合は、使用者がリーダライタQ3にパスワードを入力することによる場合は、図30に示す各工程で同じ機能をもつリーダライタを用いてセキュリティを図ることができる。

【0187】また、暗号鍵をあらかじめリーダライタQ3に設定しておいて、使用者が暗号鍵の存在を知らずに、予め非共通製品情報メモリ部Q11にアクセスできるようなリーダライタを用いた場合は、図30に示す各工程で異なるリーダライタを用いることで、各工程同士のセキュリティを図ることができる。さらに、共通製品情報を読み出す際にも、各工程で共通の暗号鍵を設定しておき、非共通製品情報を読み出す際には、各工程で

はそれぞれ共通の暗号鍵とは異なる暗号鍵（例えば、図30における各工程での第1～第5の暗号鍵）を設定しておくことで、特定の製品が流通される業界内において、各工程同士および各工程内の閉ざされた工程においてセキュリティを図ることができる。

【0188】また、第3の実施の形態においてライフサイクルの各工程において共通製品情報メモリ部Q10および非共通製品情報メモリ部Q11に書き込まれる製品情報に、書き込むことによって書き込まれたときの年月日および時刻情報を含ませておくことで、リーダライタQ3からの新たな製品情報を共通製品情報メモリ部Q10あるいは非共通製品情報メモリ部Q11に書き込む際、共通製品情報メモリ部Q10あるいは非共通製品情報メモリ部Q11に書き込まれたときの年月日および時刻情報を含めておくことで、リーダライタQ3からの新たな製品情報を共通製品情報メモリ部Q10あるいは非共通製品情報メモリ部Q11に書き込む際、その新たな製品情報が共通製品情報メモリ部Q10あるいは非共通製品情報メモリ部Q11に書き込まれたときの年月日および時刻情報を含めておくことで、リーダライタQ3からの新たな製品情報を共通製品情報メモリ部Q10あるいは非共通製品情報メモリ部Q11に書き込むことができるようすることができる。

【0189】また、リーダライタQ3の使用者にメモリ容量が不足した共通製品情報メモリ部Q10あるいは非共通製品情報メモリ部Q11に書き込まれた製品情報のリストをリーダライタQ3に送信することにより、使用者にどの製品情報を削除するかを選択させて、一番不要な製品情報を使用者の判断により削除することも可能である。

【0190】次に、自動で、例えば、共通製品情報メモリ部Q10に情報を書き込む際、共通製品情報メモリ部Q10のメモリ容量が不足しているときは、メモリの容量がある非共通製品情報メモリ部Q11に新たな製品情報を書き込むことも可能である。なお、この場合は、書き込む使用者が、共通製品情報として書き込みたいのに、非共通製品情報として書き込まれるので、このときは、書き込み不可能とするか、共通製品情報を非共通製品情報として記憶してもよいかの可否を使用者に応答することにより、セキュリティは図ることができる。

4 第4の実施の形態

次に、本発明における第4の実施の形態に係るライフサイクル管理システムについて説明する。第4の実施の形態において、ライフサイクル工程は第2の実施の形態と同じで図30を用いて説明し、第4の実施の形態のICタグの構造を図33に示し、図31と同じ構成のものには、同じ符号を付し、説明を省略する。

【0191】第4の実施の形態において、図30に示す5つの各工程における製品情報は、第2の実施の形態のものと同じである。また、各工程間のセキュリティを図る場合は、第3の実施の形態のように各工程において共通の情報として共有化された共通製品情報と、各工程同士において共有化しないで各工程内で閉ざされた非共通

製品情報とに分ける。

【0192】第4の実施の形態が第2および第3の実施の形態と異なる点は、ICタグQ2cのメモリ8cが、一回に限り書き込み可能で読み出し専用のメモリであるROM Q12と何度も読み書き可能なメモリであるRAM Q13とからなるものである。なお、セキュリティを図る場合は、図33に示すように、さらに、ROM Q12を共通製品情報を記憶する共通製品情報ROM部Q14および非共通製品情報を記憶する非共通製品情報ROM部Q15に分け、RAM Q13を共通製品情報を記憶する共通製品情報RAM部Q16および非共通製品情報を記憶する非共通製品情報RAM部Q17に分ける。なお、ROM Q12に記憶される製品情報は、主に生産工程での製品のID情報であり、各工程に共通な製品情報である。

【0193】また、ROM Q12あるいはRAM Q13のどちらかが共通製品情報を記憶するメモリ部および非共通製品情報を記憶するメモリ部を有していればセキュリティを図ることができる。次に、第4の実施の形態のICタグQ2cとリーダライタQ3の通信システムについて図33を用いて説明する。なお、第4の実施の形態では、ROM Q12およびRAM Q13のどちらもが共通製品情報を記憶するメモリ部および非共通製品情報を記憶するメモリ部を有する場合について説明する。

【0194】第4の実施の形態では、ICタグQ2cに製品情報を書き込むときに、その書き込み製品情報を、第三者が消去できないようしたいときはROM Q12に書き込み、第三者が消去できるようしたいときはRAM Q13に書き込むようにしたものである。まず、図33に示すように、ICタグQ2cに製品情報を書き込むときは、リーダライタQ3の使用者は、製品情報を共通製品情報あるいは非共通製品情報にするかを選択し、また、その製品情報が消去されてもよいかを選択して暗号化された信号をICタグQ2cに送信する。

【0195】ICタグQ2cはその暗号化された製品情報の信号をアンテナQ4で受信し、受信信号は電源回路Q5により電力に変換してICタグQ2cに電力を供給するとともに、復調回路Q6により受信信号を復調する。このとき復調された信号には、共通製品情報RAM部Q14、非共通製品情報ROM部Q15、共通製品情報RAM部Q16あるいは非共通製品情報RAM部Q17のいずれかへ書き込むかを指定するメモリ指定情報を含まれているので、そのメモリ指定情報を従って、指定されたところに、制御回路Q7により、受信信号の内容の書き込みが行われる。

【0196】次に、ICタグQ2cから共通製品情報を読み出すときは、リーダライタQ3の使用者は、リーダライタQ3から共通製品情報を読み出す信号を含む信号をICタグQ2cに送信する。アンテナQ4から受信した共通製品情報を読み出す信号は、電源回路Q5により

電力となるとともに、復調回路Q6により復調され、制御回路Q7によってメモリ8cの共通製品情報ROM部Q14あるいは非共通製品情報RAM部Q16から必要な共通製品情報を読み出し、変調回路Q9を通してアンテナQ4から電波信号として送出してリーダライタQ3で共通製品情報を受信する。

【0197】また、ICタグQ2cから非共通製品情報を読み出すときは、まず、リーダライタQ3の使用者は、非共通製品情報RAM部Q15あるいは非共通製品情報ROM部Q16をアクセスするために非共通製品情報RAM部Q17を指すための暗号鍵を入力する。リーダライタQ3は、アンテナQ4から受信した非共通製品情報を読み出す信号は、電源回路Q5により電力となるとともに、復調回路Q6により復調され、制御回路Q7によって非共通製品情報RAM部Q15あるいは非共通製品情報RAM部Q16から必要な非共通製品情報を読み出す。

【0198】そして、暗号鍵により非共通製品情報を読み出しが可能となったとき、リーダライタQ3から必要な非共通製品情報を読み出す信号をICタグQ2cに送信する。アンテナQ4から受信した非共通製品情報を読み出す信号は、電源回路Q5により電力となるとともに、復調回路Q6により復調され、制御回路Q7によって非共通製品情報RAM部Q17あるいは非共通製品情報RAM部Q16から必要な非共通製品情報を読み出す。

【0199】読み出された非共通製品情報の信号は変調回路Q9を通してアンテナQ4から電波信号としてリーダライタQ3へ送信される。第4の実施の形態は、第3の実施の形態と同様に、少なくとも非共通製品情報ROM部Q15あるいは非共通製品情報RAM部Q17に書き込まれた非共通製品情報を読み出すときは、リーダライタQ3からICタグQ2cに送信する読み出し信号に非共通製品情報メモリ部Q11を指定する信号、すなわち暗号鍵が含まれていないと制御回路Q7が判断した場合は、その読み出し信号は、メモリ8cにアクセスできないようにブロックされているものである。

【0200】各工程における各リーダライタはそれぞれ別の暗号鍵をもっているため、この暗号鍵の存在により、特定の使用者のみが非共通製品情報を得ることができるシステムとなっている。なお、第4の実施の形態において、この暗号鍵は、非共通製品情報RAM部Q15あるいは非共通製品情報RAM部Q17の非共通製品情報を読み出すための信号を意味し、使用者がリーダライタQ3にパスワードを入力することによる信号の場合は、図30に示す各工程同士で同じ機能をもつリーダライタQ3を用いてセキュリティを図ることができる。

【0201】また、暗号鍵をあらかじめリーダライタQ3に設定しておいて、使用者が暗号鍵の存在を知らずに、他の非共通製品情報RAM部Q15あるいは非共通製品情報RAM部Q17をアクセスできるようなリーダライタを用いた場合は、図30に示す各工程同士で異なったリーダライタを用いることで、各工程同士のセキュリティを図ることができる。

【0202】さらに、共通製品情報を読み出す際にも各工程で共通の共通製品情報RAM部Q14あるいは共通製品情報RAM部Q16のそれぞれに対応する第1の暗号鍵、第2の暗号鍵を設定しておき、非共通製品情報を読み出す際は、非共通製品情報ROM部Q15あるいは非共通製品情報RAM部Q17のそれぞれに対応した各工程で異なる複数の暗号鍵を設定しておくことで、各工程内の閉ざされた工程においてもセキュリティを図ることができる。

【0203】また、第4の実施の形態においてライフルサイクルの各工程において、共通製品情報RAM部Q16および非共通製品情報RAM部Q17のメモリ部に書き込まれる製品情報に、書き込むごとに書き込まれたときの年月日および時刻情報を記させておくことで、リーダライタQ3からの新たな製品情報をこれらのRAMのメモリ部に書き込む際、これらのRAMのメモリ部どれかのメモリの容量が不足して、その新たな製品情報がその容量不足のメモリ部に書き込むことができないときは、そのRAMのメモリ部の最も古い製品情報を自動で削除して、新たな製品情報をRAMのメモリ部に書き込むことができるようになることができる。

【0204】また、リーダライタQ3の使用者にメモリ容量が不足したメモリ部に書き込まれた製品情報のリストをリーダライタQ3に送信することにより、使用者にどの製品情報を削除するかを選択させて、一番不要な製品情報を使用者の判断により削除して、その指定のメモリ部に書き込むようになることも可能である。次に、自動で、例えば、共通製品情報RAM部Q16に情報を書き込む際に共通製品情報RAM部Q16のメモリ容量が不足しているときは、メモリの容量がある非共通製品情報RAM部Q17に新たな製品情報を書き込むことも可能である。

【0205】なお、この場合は、書き込む使用者が、共通製品情報として共通製品情報RAM部Q16に書き込みたいのに、非共通製品情報として非共通製品情報RAM部Q17に書き込まれるので、このときは、書き込み不可能とするか、共通製品情報を非共通製品情報として記憶してもよいかの可否を使用者に応答することにより、また、メモリ容量に余裕のある非共通製品情報RAM部Q17に、自動あるいは使用者に選択させることにより、セキュリティを図ることができる。なお、RAM部について説明したが、ROM部においても同様のことができる。

【0206】また、例えば、ROM部に製品情報を書き込む際に、ROM Q12のメモリ容量が不足しているときには、メモリ容量のあるRAM Q13に新たな製品情報を書き込むことも可能である。この場合、ROM Q12とRAM Q13において、共通製品情報は共通製品情報として扱い、非共通製品情報は非共通製品情報として扱うのが好ましいが、これに限らない。

5 第5の実施の形態

次に、本発明における第5の実施の形態に係るライフサイクル管理システムについて説明する。第5の実施の形態において、ライフサイクル工程は第2の実施の形態と同じなので図30を用いて説明し、第4の実施の形態のICタグの構造を図34に示し、図31と同じ構成のものには同じ符号を付し、説明を省略する。

【0207】第5の実施の形態が第2、第2および第4の実施の形態と異なる点は、図34(a)に示すよう

- 10 に、ICタグQ2dのメモリ8dが、図30に示す工程の数だけ分けられ、それぞれ生産工程Q23の製品情報を記憶する第1のメモリ部Q18、物流工程Q24の製品情報を記憶する第2のメモリ部Q19、販売工程Q25の製品情報を記憶する第3のメモリ部Q20、使用工程Q26の製品情報を記憶する第4のメモリ部Q21および回収処理工程Q27の製品情報を記憶する第5のメモリ部Q22に分けられていることである。なお、工程数に応じて必要な工程の数だけメモリを分ければよい。

- 【0208】第5の実施の形態において、図30に示す20 5つの各工程における製品情報は、第2の実施の形態で説明したのと同じである。また、各工程間のセキュリティを図る場合は、図34(b)に示すように、第3の実施の形態のよう各工程において共通の情報として共有化された共通製品情報と、各工程同士において共有化しないで各工程内で閉ざされた非共通製品情報とに分け、第1～第5のメモリ部Q18～Q22を、それぞれ共通製品情報メモリ部と非共通製品情報メモリ部に分ければよい。

- 【0209】また、第4の実施の形態に示したように、30 さるに、第1～第5のメモリ部Q18～Q22を、ROMとRAMに分けて、ROMを共通製品情報を記憶する共通製品情報RAM部および非共通製品情報を記憶する非共通製品情報RAM部に分け、RAMを共通製品情報を記憶する共通製品情報RAM部および非共通製品情報を記憶する非共通製品情報RAM部に分けてセキュリティを図ることができる(図示せず)。

- 【0210】次に、図34(b)を用いて、第5の実施の形態のICタグQ2dとリーダライタQ3の通信システムについて説明する。まず、図34(b)において、40 第1の工程においてICタグQ2dに製品情報を書き込むときは、第1の工程内のリーダライタQ3の使用者は、製品情報を共通製品情報あるいは非共通製品情報にするかを選択して暗号化された信号をICタグQ2dに送信する。

- 【0211】ICタグQ2dはその暗号化された製品情報の信号をアンテナQ4で受信し、受信信号は電源回路Q5により電力に変換してICタグQ2dに電力を供給するとともに、復調回路Q6により受信信号を復調化する。このとき復調化された信号には、第1のメモリ部Q50 18の共通製品情報メモリ部あるいは非共通製品情報メ

モリ部のいすれかへ書き込むを指定するメモリ指定情報が含まれるので、そのメモリ指定情報に従って、指定されたところに、制御回路Q7により、受信信号の内容の書き込みが行われる。

【0212】次に、第1の工程内にICタグQ2dから共通製品情報を読み出すときは、リーダライタQ3の使用者は、リーダライタQ3から共通製品情報を読み出す信号を含む信号をICタグQ2dに送信する。アンテナQ4から受信した共通製品情報を読み出す信号は、電源回路Q5により電力となるとともに、復調回路Q6により復調され、制御回路Q7によって第1のメモリ部Q18の共通製品情報メモリ部から必要な共通製品情報を読み出し、変調回路Q9を通してアンテナQ4から電波信号として送出してリーダライタQ3で共通製品情報を受信する。

【0213】また、図34において、ICタグQ2dから非共通製品情報を読み出すときは、まず、非共通製品情報を書き込まれた工程が第1の工程の場合は、リーダライタQ3の使用者は、第1のメモリ部Q18の非共通製品情報メモリ部にアクセスするために第1のメモリ部Q18の非共通製品情報メモリ部を指定する信号、すなわちその工程専用暗号鍵をICタグQ2dに送信する。

【0214】そして、工程専用暗号鍵により非共通製品情報を読み出しが可能となったとき、リーダライタQ3から必要な非共通製品情報を読み出す信号をICタグQ2dに送信する。そして、アンテナQ4から受信した非共通製品情報を読み出す信号は、電源回路Q5により電力となるとともに、復調回路Q6により復調され、制御回路Q7によって第1のメモリ部の非共通製品情報メモリ部から必要な非共通製品情報を読み出される。

【0215】読み出された非共通製品情報の信号は変調回路Q9を通してアンテナQ4から電波信号として送信され、リーダライタQ3で非共通製品情報を受信する。また、第5の実施の形態において、例えば第1の工程でメモリの容量が不足したときは、第1のメモリ部のメモリ容量の範囲で、第3、第4の実施の形態で説明したように、自動で製品情報を消去したり、使用者にどの製品情報を削除するかを選択させて、一番不要な製品情報を使用者の判断により削除するものである。

【0216】このように第5の実施の形態では、メモリが工程数の数だけ分けられているので、ICタグには、各工程の製品情報が記憶されているものの、各工程内でセキュリティを図ることができる。以上、第2～第5の実施の形態で用いられたICタグは、搬送周波数として8.60～9.15MHzのUHF帯、2.4～2.5GHzの準マイクロ波帯を用い、電磁結合を用いた磁気方式ではなく、電波方式を用いて通信を行っている。

【0217】磁気方式の周波数は、1.25kHzや1.3.5MHzが知られており、電波方式よりも、周波数

が高くない。これにより、電波方式は、磁気方式よりも高周波であるのでアンテナを小さくできるのでタグ寸法を小型化できることともに、低コストにもできる。また、通信距離に関しては、磁気方式は、数十cmだが、電波方式では、數mになる。

【0218】また、通信距離に関しては、磁気方式は、數kbpsだが、電波方式では、數十kbpsと高速化することができる。また、磁気方式は、コイルなどの電磁結合によるものなので、磁気方式の情報記憶媒体が複数個重なっていると、重要なものは通信遮断されることもあり、その重ね読みはICカードでは枚数程度であるが、電波方式は、一度に數十枚の重ね読みが可能で、その電波は、段ボール等の紙、プラスチック、陶器、衣服などの繊維などの、水あるいは金属以外のものをほとんど損失無く通過することができる。

【0219】これにより、一度に同じあるいは異なる種類の製品の製品情報を読み出すこともでき、また、一度に同じ種類の製品に同じ製品情報を書き込むこともできるので、リーダライタの使用者は、ICタグへの製品情報の書き込みまたは読み出しを容易に行うことができる。例えば、周波数を9.15/8.68MHzでタグ寸法を5mm×100mm×0.5mmとしたICタグの場合、読み出し距離が約3m、書き込み距離が約2m、読み出し速度は約1.0m秒/バイト、書き込み速度は約2.0m秒/バイトとなる。

【0220】また、周波数を2.45GHzでタグ寸法を5mm×30mm×0.5mmとしたICタグの場合には、読み出し距離が約1.5m、書き込み距離が約1m、読み出し速度は約1.0m秒/バイト、書き込み速度は約2.0m秒/バイトとなる。本発明によれば、製品にICタグを取り付けることにより、製品の履歴情報をそのままに記憶させることで、各ライフサイクル工程において、次のような効果がある。

【0221】生産工程においては、生産台数の管理を行うことができ、生産調整を容易に行うことができる。また、製品あるいは部品を回収して製品情報を解析することにより、開発、設計にフィードバックすることができ、製品あるいは部品の性能の向上を図ることができ。また、物流工程においては、在庫管理が容易になります。

【0222】また、販売工程においては、在庫を減らすことができる。また、種々の製品が混ざれても、一度に種々の製品をリーダライタにより容易に管理ができるので、効率的な輸送が期待できとともに、誤った配送も減らすことができる。

【0223】また、販売工程においては、万引き防止、売れ筋商品の把握、容易な在庫管理等の効果が期待できる。また、使用工程においては、点検サービスや修理などを信頼性をもって実施することができる。また、回収工程においては、製品あるいは部品の再利用の評価をすることができるので、有効にリサイクルが行える。

【0223】さらに、製品の履歴情報が残っているので

消費者保護法（PL法）の対策にもなる。尚、本発明は、本実施の形態に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0224】また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピー（登録商標）ディスク、ハードディスク、CD-ROM、MO、DVD、D VD-ROM、DVD-RAM、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0225】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。更に、本発明は、上記に示す実施の形態、複数の変形例、又は上記実施の形態及び複数の変形例の一部を組み合わせるとしてもよい。

【図面の簡単な説明】

【図1】生産1、物流2、販売3、サービス4、回収リサイクル5の各ステージを経て流れ、その一生を終える。製品の生産から廃棄・回収に至るまでの製品のライフサイクル6を示す。

【図2】テレビ受像機の前面枠部分に、無線ICタグが貼り付られ、無線ICタグの上面に、ロゴマークが貼り付けられている状態を示す。

【図3】無線ICタグが貼り付けられたラベルが衣服の襟裏側部に貼り付けられている状態を示す。

【図4】ライフサイクル管理システム10の構成を示すブロック図である。

【図5】サブシステム20の構成を示すブロック図である。

【図6】生産管理サブシステム20aに含まれる第1組のリーダライタ30a及び管理装置40aが、生産工場内に設置されている状況を示す。

【図7】物流管理サブシステム20bに含まれる第3組のリーダライタ30d及び携帯電話内蔵型管理装置40dが、貨物トラックに搭載されている様子を示す。

【図8】物流管理サブシステム20bに含まれる第2組の携帯電話型リーダライタ30cの外観を示す。

【図9】販売管理サブシステム20cに含まれる第1組のリーダライタ30bの外観を示す。

【図10】サービス管理サブシステム20dに含まれる第4組の携帯端末型リーダライタ30eの外観を示す。

【図11】リーダライタ30の構成を示すブロック図である。

【図12】同期信号送信期間、識別コード収集期間及び

アクセス期間を示す。

【図13】命令生成部104が受け取る命令とこれらの命令に付随するオペランド等を示す。

【図14】命令解読部110が抽出する命令とオペランドなどを示す。

【図15】無線ICタグ80の外観を示す。

【図16】無線ICタグ80のICチップ部200の構成を示すブロック図である。

【図17】メモリ部216の構成を示すメモリマップである。

【図18】メモリ部216の構成を示すメモリマップである。メモリ部216の内容をステージ領域毎に示している。

【図19】電源部203に含まれる電源回路の一例を示す。

【図20】認証部210の構成を示すブロック図である。

【図21】管理装置40の構成及びホストコンピュータ60の構成を示すブロック図である。

【図22】ホストコンピュータ60のデータベース61に記憶されている情報の一例を示す。

【図23】リーダライタ30及び無線ICタグ80の概要動作を示すフローチャートである。

【図24】無線ICタグの識別コードの収集の動作を示すフローチャートである。

【図25】無線ICタグの領域アクセス認証と領域アクセスの動作を示すフローチャートである。

【図26】無線ICタグの適用分野と、タグ単価と、通信距離の関係を示す。

【図27】リーダライタ30と同様のリーダライタを内蔵している家庭用電気洗濯機の外観図である。

【図28】拡張領域を含むメモリ部のメモリマップの一例である。

【図29】リーダライタが1個の無線ICタグのみに対して読み書きを行う場合の、ステージ領域の認証とステージ領域へのアクセスの動作を示すフローチャートである。

【図30】本発明のライフサイクル管理システムのライフサイクル工程を示す図である。

【図31】本発明の第2の実施の形態に係る非接触のICタグの構造およびリーダライタを示すブロック図である。

【図32】本発明の第3の実施の形態に係る非接触のICタグの構造およびリーダライタを示すブロック図である。

【図33】本発明の第4の実施の形態に係る非接触のICタグの構造およびリーダライタを示すブロック図である。

【図34】本発明の第5の実施の形態に係る非接触のICタグの構造およびリーダライタを示すブロック図であ

る。

る。

【符号の説明】

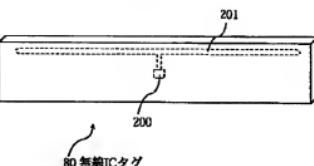
1 生産	107 録記憶部
2 物流	108 暗号化部
3 販売	109 ハッシュ部
4 サービス	110 命令解読部
5 回収リサイクル	111 変復調部
6 製品のライフサイクル	112 アンテナ部
10 ライフサイクル管理システム	200 ICチップ部
20 サブシステム	201 アンテナ部
20a 生産管理サブシステム	10 203 電源部
20b 物流管理サブシステム	206 循調部
20c 販売管理サブシステム	207 命令解読部
20d サービス管理サブシステム	208 識別コード記憶部
20e 回収リサイクル管理サブシステム	209 制御部
30 インターネット	210 認証部
30a~30e リーダライタ	211 亂数生成部
40a~40d 管理装置	212 ハッシュ部
50 基地局	213 変調部
51 受信装置	214 クロック生成部
52 ICカード	20 215 入出力部
53 接続装置	216 メモリ部
60 ホストコンピュータ	235 比較器
61 データベース	231 録記憶部
70 LAN装置	232 亂数記憶部
80, 80a, 80b 無線ICタグ	233 暗号化部
81 テレビ受像機 82 の前面枠部分	234 生成乱数記憶部
82 テレビ受像機	235 比較器
83 ロゴマーク	301 非プロトクト部
93 ラベル	302 プロトクト部
90 衣服	30 401 情報記憶部
91 標識剥離部	402 制御部
101 入出力部	403 LAN接続部
102 制御部	404 入出力部
103 一時記憶部	601 制御部
104 命令生成部	602 LAN接続部
105 クロック生成部	603 DB更新部

*

【図14】

命令種別	オペランド等
識別コード送信命令	乱数R0, 識別コード
認証子送信命令	識別コード、認証子
識別コード一致命令	識別コード
アクセス応答命令	識別コード、アクセス応答情報
アクセス不許可命令	識別コード、理由コード

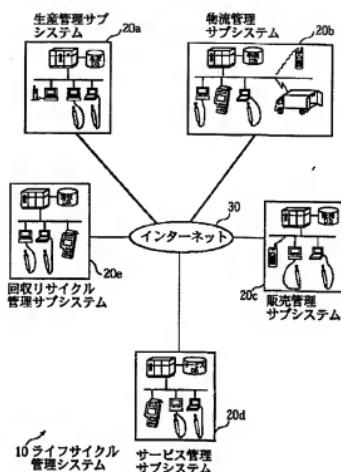
【図15】



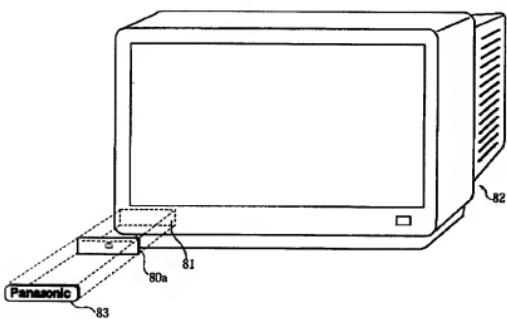
【図1】



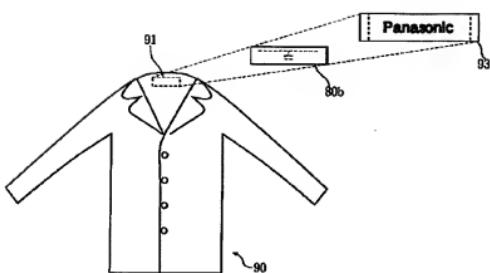
【図4】



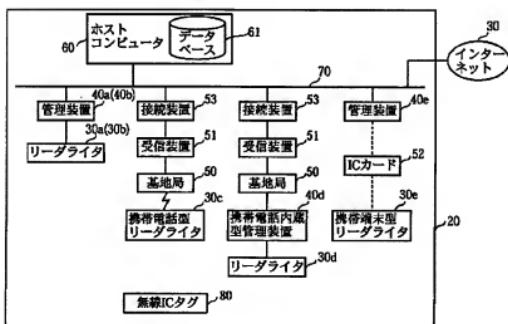
【図2】



【図3】



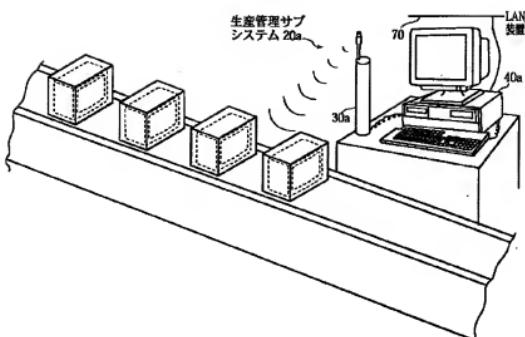
【図5】



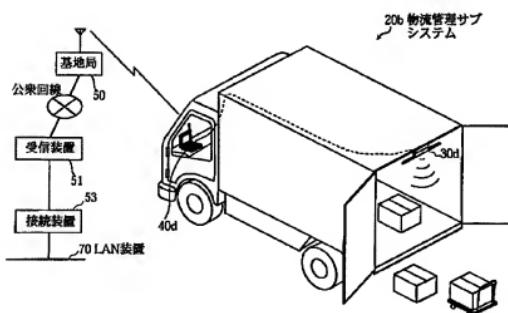
【図13】

命令種別	オペランド等
同期信号送信命令	同期信号
識別コード収集命令	
アクセス要求命令	識別コード
アクセス命令	
Read 命令	識別コード、物理アドレス、読み出しバイト数
Write 命令	識別コード、物理アドレス、書込みバイト数、書込み内容
識別コード応答命令	識別コード
認証子応答命令	識別コード、認証子

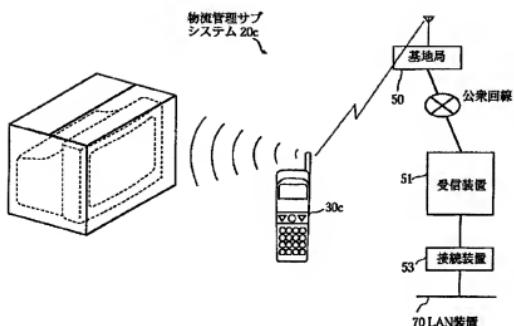
【図6】



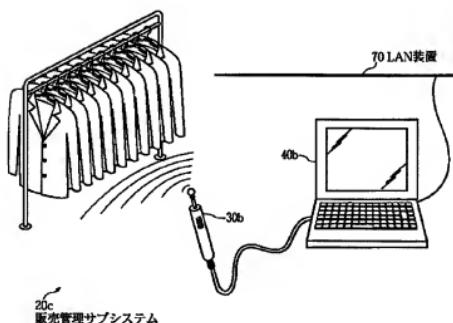
【図7】



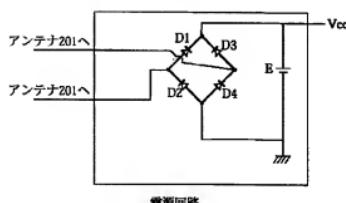
【図8】



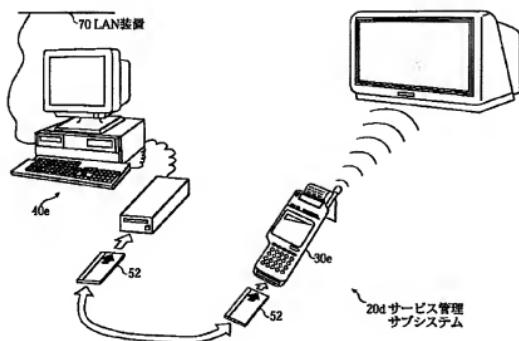
【図9】



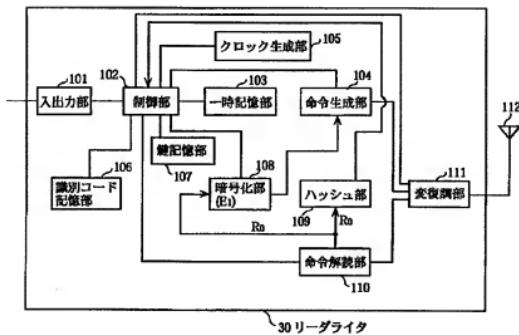
【図19】



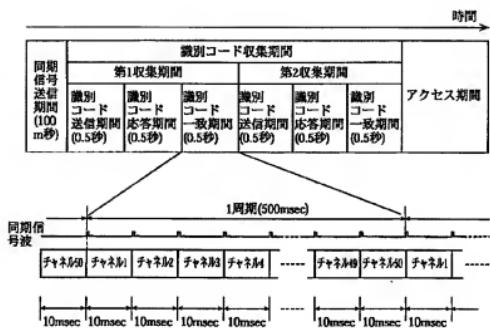
【図10】



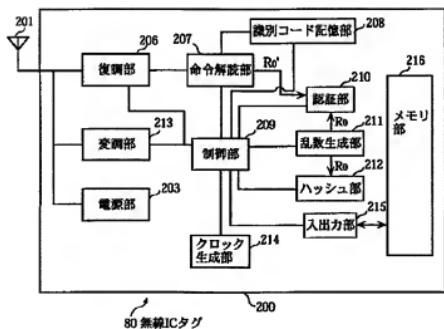
【図11】



【図12】



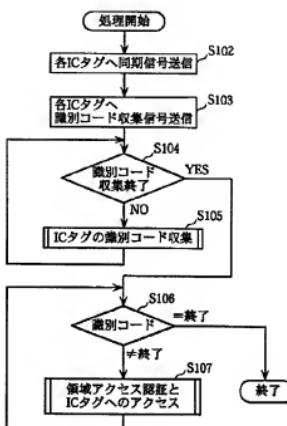
【図16】



[圖 17]

アドレス	
311	0 50バイト
312	49 50バイト
313	99 100 50バイト
314	149 150 198 200 50バイト
315	249 250
321	399 400 150バイト
322	549 550 150バイト
323	699 700 150バイト
324	849 850 150バイト
325	999 バイト

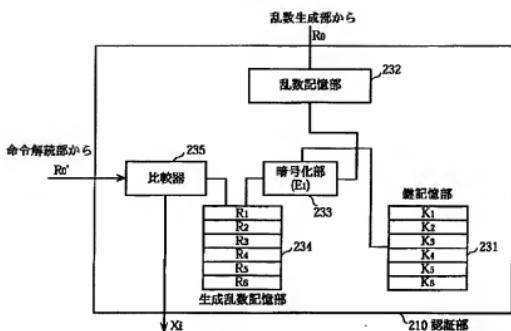
〔図23〕



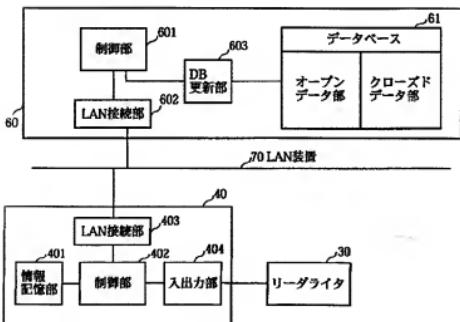
【図18】

	生産ステージ 領域	物流ステージ 領域	販売ステージ 領域	サービスステージ 領域	回収リサイクル ステージ領域
非プロ ダクト部	メカ名	運送業者名	保証期間	洗濯方法	
301	品名		保証番号		
	製番	入出庫日	卸業者名		回収業者 回収日
アコ外 部	製造日	GLN(アーバン ワールド番号)	小売店名		高業者者 原発日
302	工場名		販売日	修理者名 修理日 修理部品	リユース記録 可変部

【図20】



【図21】

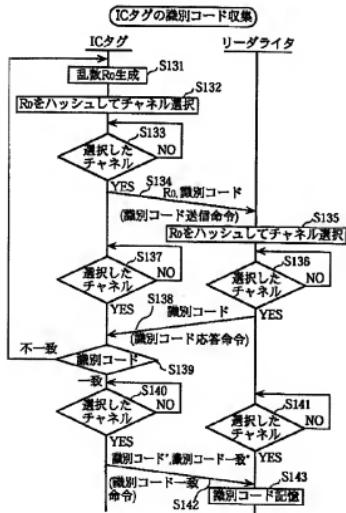


【図22】

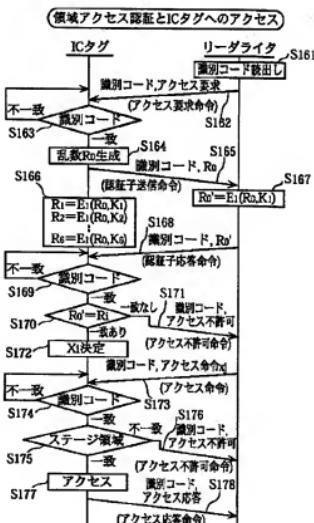
データ部	生産データ部	物流データ部	販売データ部	サービスデータ部	回収サイクルデータ部
分解方法					リサイクル活用情報
部品データ					
有毒情報					

検査情報	追跡記録	POS情報	品質情報	マーチスト情報
部品データ				
有毒情報				
クローズドデータ部		販売先情報		

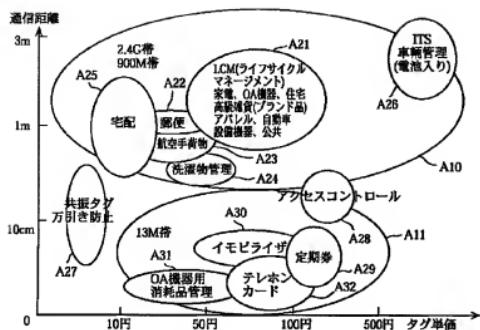
【図24】



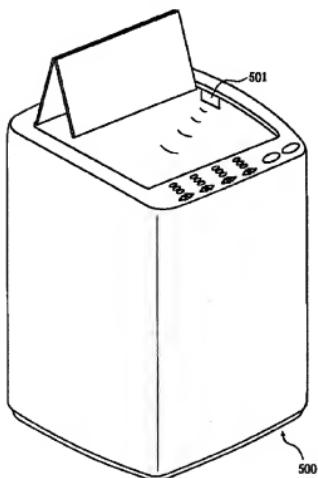
【図25】



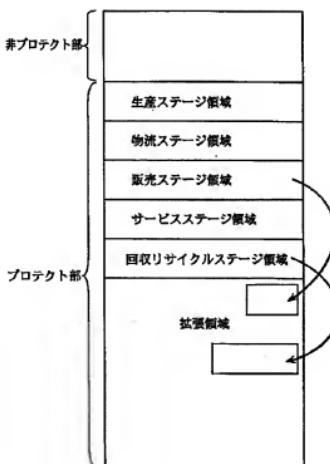
【図26】



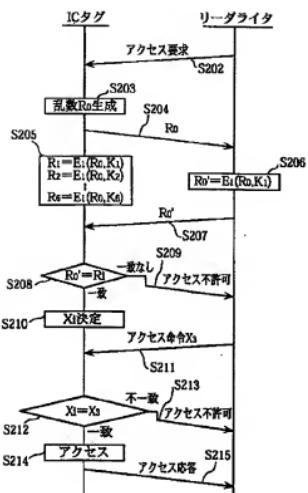
【図27】



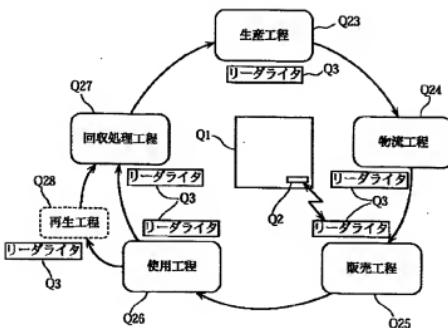
【図28】



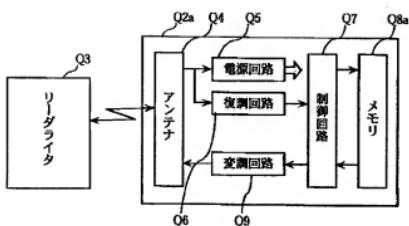
【図29】



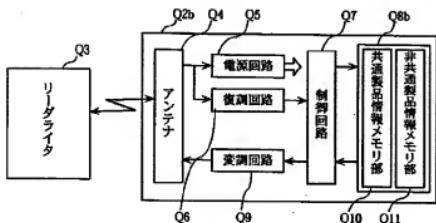
【図30】



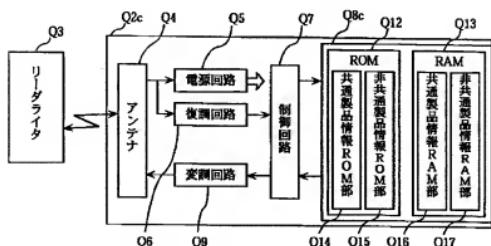
【図31】



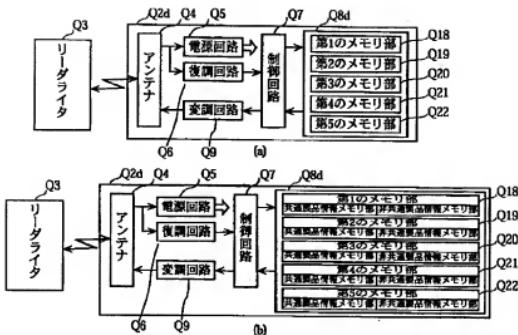
【図32】



【図33】



【図34】



フロントページの続き

(51)Int.CI.⁷
G 0 6 K 19/07
19/00

識別記号

F I
G 0 6 K 19/00

コード(参考)
H
Q

F ターム(参考) 2C005 MA01 MB01 MB06 MB10 NA08
SA02 SA22 SA25 TA22
5B035 AA13 BB09 CA23 CA38
5B058 CA17 KA35 YA20

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成15年5月23日(2003.5.23)

【公開番号】特開2001-307055(P2001-307055A)

【公開日】平成13年11月2日(2001.11.2)

【年通号数】公開特許公報13-3071

【出願番号】特願2000-388796(P2000-388796)

【国際特許分類第7版】

G06K 19/073

B42D 15/10 521

G06K 17/00

19/07

19/00

[F1]

G06K 19/00 P

B42D 15/10 521

G06K 17/00 F

L

E

19/00 H

Q

【手続補正書】

【提出日】平成15年2月7日(2003.2.7)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 不揮発性メモリを有し、電波を用いて非接触に読み書き可能な情報記憶媒体であって、

複数の記憶領域を有する記憶手段と、

各記憶領域を識別する領域識別子を格納している格納手段と、

外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、

受信した前記アクセス識別子が前記記憶手段に格納されている領域識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、

受信したアクセス情報を基づいて、前記アクセス識別子により識別される記憶領域へのアクセスを行う入出力手段とを備えることを特徴とする情報記憶媒体。

【請求項2】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを通過する物品に付され、不

揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、

前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、

前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、

外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、

受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報を基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段とを備えることを特徴とする非接触ICタグ。

【請求項3】 前記秘密受信手段は、

第1認証子を生成し、生成した第1認証子を前記アクセス装置へ出力する認証子出力手段と、

前記アクセス識別子を暗号化して用いて、出力した前記第1認証子に暗号アルゴリズムが施されて生成された第2認証子を前記アクセス装置から取得する取得手段と、

前記複数のステージ識別子を暗号化鍵として用いて、生成した前記第1認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第3認証子を生成する暗号手段とを含み、

前記判断手段は、取得した第2認証子が生成した複数の第3認証子のうちのいずれか1個と一致するか否かを判断し、一致する場合に、受信した前記アクセス識別子が前記識別子記憶手段に格納されているステージ識別子の、いざれかと一致すると判断し、

前記入出力手段は、前記アクセス識別子により識別されるステージ記憶領域として、前記第2認証子に一致する第3認証子を生成する際に暗号化鍵として用いたるステージ識別子により識別されるステージ記憶領域へのアクセスを行うことを特徴とする請求項2記載の非接触ICタグ。

【請求項4】 入院から退院に至るまでの病院の療養サイクルにおける複数のステージを経由する入院患者に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、前記療養サイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、

外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子の、いざれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報を基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行いう入出力手段とを備えることを特徴とする非接触ICタグ。

【請求項5】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流逝する高級ブランド品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子の、いざれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報を基づいて、前記アクセス識別子

により識別されるステージ記憶領域へのアクセスを行いう入出力手段とを備えることを特徴とする非接触ICタグ。

【請求項6】 不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別される複数個の記憶領域を有し、電波を用いて非接触に読み書き可能な情報記憶媒体に対して情報を送受信するアクセス装置であって、

アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記情報記憶媒体に対して送信する秘密送信手段と、前記情報記憶媒体により、秘密に送信した前記アクセス識別子が前記記憶媒体が有する複数個の記憶領域うちの1個の記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備えることを特徴とするアクセス装置。

【請求項7】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流逝する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフザイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触ICタグに対して情報を送受信するアクセス装置であって、

アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記非接触ICタグに対して送信する秘密送信手段と、前記非接触ICタグにより、秘密に送信した前記アクセス識別子が前記非接触ICタグが有する複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備えることを特徴とするアクセス装置。

【請求項8】 前記非接触ICタグは、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶しており、

前記秘密送信手段は、前記非接触ICタグから第1認証子を受信する認証子受信手段と、前記アクセス識別子を暗号鍵として用いて、受信した前記第1認証子に暗号アルゴリズムを施して第2認証子を生成し、生成した第2認証子を前記非接触ICタグへ出力する認証子出力手段とを備え、

前記アクセス情報送信手段は、前記非接触ICタグにより、前記複数のステージ識別子を暗号化鍵として用いて、前記第1認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第3認証子が生成され、出力された前記第2認証子が生成した複数の第3認証子のうちの、いざれか1個と一致するか否か判断され、一致する場合に、前記アクセス識別子が前記複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断されるときに、さらにアクセス情報を送信す

ることを特徴とする請求項7記載のアクセス装置。

【請求項9】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密のステージ識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触ICタグに対して情報を送受信するアクセス装置であって、アクセス識別子を受け付ける識別子受け付手段と、

前記アクセス識別子を暗号を用いて秘密に前記非接触ICタグに対して送信する秘密送信手段と、

前記非接触ICタグにより、秘密に送信した前記アクセス識別子が前記非接触ICタグが有する複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備えることを特徴とするアクセス装置。

【請求項10】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能であり、前記ライフケイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段とを備える非接触ICタグにより用いられる入出力方法であって、外部のアクセス装置から暗号を用いてアクセス識別子を

秘密に受信する秘密受信ステップと、

受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断ステップと、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信ステップと、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力ステップとを含むことを特徴とする入出力方法。

【請求項11】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密のステージ識別子によりそれぞれ識別されライフケイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触ICタグに対して情報を送受信し、アクセス識別子を記憶している識別子記憶手段を備えるアクセス装置により用いられるアクセス方法であって、

前記アクセス識別子を暗号を用いて秘密に前記非接触ICタグに対して送信する秘密送信ステップと、

前記非接触ICタグにより、秘密に送信した前記アクセス識別子が前記非接触ICタグが有する複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信ステップとを含むことを特徴とするアクセス方法。